ЭНЦИКЛОПЕДИЯ ЭЛЕМЕНТАРНОЙ МАТЕМАТИКИ

I

ЭНЦИКЛОПЕДИЯ ЭЛЕМЕНТАРНОЙ МАТЕМАТИКИ

I

АРИФМЕТИКА

АКАДЕМИЯ ПЕДАГОГИЧЕСКИХ НАУК РСФСР

ЭНЦИКЛОПЕДИЯ ЭЛЕМЕНТАРНОЙ МАТЕМАТИКИ

ПОД РЕДАКЦИЕЙ
П. С. АЛЕКСАНДРОВА,
А. И. МАРКУШЕВИЧА
и А. Я. ХИНЧИНА

КНИГА ПЕРВАЯ

АРИФМЕТИКА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1951 ЛЕНИНГРАД

11-5-2

Редактор *А. З. Рывкин.* Техн. редактор *Н. Я. Мурашова.*

Подписано к печати 12/XII 1950 г. Бумага 60×92¹/₁₆. 14 бум. л. 28 печ. л. 30,11 уч.-изд. л. 44.444 печ. знак. в печ. л. Т-09193. Тираж 50000 экз. Цена книги 10 р. 55 к. Переплёт 2 р. Заказ № 875.

2-я типография «Печатный Двор» им. А. М. Горького Главполиграфиздата при Совете Министров СССР. Ленинград, Гатчинская. 26.

ОГЛАВЛЕНИЕ

Предисловие 6

ПРОИСХОЖДЕНИЕ СИСТЕМ СЧИСЛЕНИЯ

(И. Г. Башмакова и А. П. Юшкевич)

Введение 11

§ 1. Начальная стадия развития счёта 15
§ 2. Непозиционные системы счисления 27
§ 3. Алфавитные системы нумерации 31
§ 4. Поместные или позиционные системы счисления 38
§ 5. Распространение позиционного принципа записи чисел в Западной Европе и в России 50
§ 6. Дроби 57

Заключение 72

ПОНЯТИЯ МНОЖЕСТВА, ГРУППЫ, КОЛЬЦА И ПОЛЯ. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АРИФМЕТИКИ

(И. В. Проскуряков)

Введение 77

Глава I. **Множества** 80

§ 1. Понятие о множестве 80
§ 2. Операции над множествами 82
§ 3. Функция, отображение, мощность 84
§ 4. Конечные и бесконечные множества 89
§ 5. Упорядоченные множества 95

Глава II. **Группы, кольца и поля** 100

§ 6. Группа 100
§ 7. Кольцо 108
§ 8. Поле 113
§ 9. Аксиоматическое построение математики. Изоморфизм . . . 120
§ 10. Расположенные кольца и поля 125

Глава III. **Натуральные числа** 133

§ 11. Аксиомы натуральных чисел 133
§ 12. Сложение 135
§ 13. Умножение 139
§ 14. Порядок 142
§ 15. Индуктивные определения. Сумма и произведение нескольких чисел 145
§ 16. Вычитание и деление 150
§ 17. Замечания о системе аксиом натуральных чисел 152

Глава IV. **Кольцо целых чисел** 157
§ 18. Принцип расширения в арифметике и алгебре 157
§ 19. Эквивалентность и разбиение на классы 159
§ 20. Определение кольца целых чисел 160
§ 21. Свойства целых чисел 168

Глава V. **Поле рациональных чисел** 172
§ 22. Определение поля рациональных чисел 172
§ 23. Свойства рациональных чисел 179

Глава VI. **Поле действительных чисел** 188
§ 24. Полные и непрерывные поля 188
§ 25. Определение поля действительных чисел 202
§ 26. Свойства действительных чисел 214
§ 27. Аксиоматическое определение действительных чисел 222

Глава VII. **Поле комплексных чисел** 227
§ 28. Определение поля комплексных чисел 227
§ 29. Свойства комплексных чисел 233
§ 30. Гиперкомплексные числа, кватернионы 241

Литература 252

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

(А. Я. Хинчин)

Глава I. **Делимость и простые числа** 255
§ 1. Введение 255
§ 2. Однозначное разложение чисел на простые множители . . . 256
§ 3. О простых числах 262

Глава II. **Метод сравнений** 271
§ 4. Введение 271
§ 5. Сравнения и их основные свойства 272
§ 6. Классификация чисел по данному модулю 277
§ 7. Сравнения, содержащие неизвестные 282

Глава III. **Алгорифм Евклида и цепные дроби** 291
§ 8. Алгорифм Евклида 291
§ 9. Элементарная теория цепных дробей 297

Глава IV. **Представление чисел систематическими и цепными дробями** 307
§ 10. Введение 307
§ 11. Систематические дроби 308
§ 12. Цепные дроби 315

Глава V. **Цепные дроби и диофантовы приближения** 322
§ 13. Подходящие дроби в роли наилучших приближений 322
§ 14. Диофантовы приближения 335

Глава VI. **Алгебраические и трансцендентные числа** 342
§ 15. Теорема Лиувилля и первое появление трансцендентных чисел 342
§ 16. Метод Кантора 347
§ 17. Арифметическая природа классических постоянных 349

Литература 352

УСТНЫЙ И ПИСЬМЕННЫЙ СЧЁТ. ВСПОМОГАТЕЛЬНЫЕ СРЕДСТВА ВЫЧИСЛЕНИЙ

(В. М. Брадис)

Глава I. **Общие сведения о счёте и приближённых вычислениях** 357
§ 1. Общие соображения об изучении счёта в школе 357
§ 2. Счёт устный 359
§ 3. Счёт письменный 362
§ 4. Вспомогательные средства вычисления 365
§ 5. Приближённые значения 377
§ 6. Различные способы оценки точности приближённых значений. 380
§ 7. Обработка результатов измерений 383
Глава II. **Учёт погрешностей** 388
§ 8. Вычисления со строгим учётом погрешностей по способу границ 388
§ 9. Вычисления со строгим учётом погрешностей по способу границ погрешностей 392
§ 10. Предельные погрешности результатов действий над приближёнными значениями. Правила подсчёта цифр 400
§ 11. Средние квадратические погрешности результатов действий над приближёнными числами. Принцип академика А. Н. Крылова 405
§ 12. Распределение погрешностей в результатах вычислений . . 411
§ 13. Практические применения правил подсчёта цифр. Сводка этих правил 413
Глава III. **Различные вопросы** 421
§ 14. Приближённые формулы. Сокращённые приёмы действий . 421
§ 15. Математические таблицы 427
§ 16. Графические вычисления 429
§ 17. Счётная логарифмическая линейка 431
§ 18. Вычислительная работа в разные годы обучения 437
Литература 441
Алфавитный указатель 442

ПРЕДИСЛОВИЕ

Издание «Энциклопедии элементарной математики» задумано Академией педагогических наук РСФСР как пособие для учителей математики средней школы и студентов физико-математических факультетов педагогических и учительских институтов. Его назначение — дать систематическое изложение научных основ школьного предмета математики. Отсюда вытекают особенности этого издания. Прежде всего труд этот не может служить для первоначального изучения предмета. Он предназначается для людей, изучавших элементарную математику и уже ставших или готовящихся стать преподавателями элементарной математики. Он не следует, как правило, ни порядку, ни способу изложения математики в средней школе, так как то и другое обусловлено возрастными особенностями учащихся и общеобразовательными целями средней школы, т. е. соображениями, которые не играют роли по отношению к подготовленному читателю-профессионалу. Логика нашего издания — это логика систематического, по возможности простого и доступного, изложения тех вопросов математической науки, из которых строится школьный курс, а также и тех, которые хотя и не находят в этом курсе прямого выражения, однако необходимы для правильного и сознательного его понимания и создают перспективы для дальнейшего развития содержания и методов школьного курса.

Всё издание рассчитано на 7 книг объёмом от 350 до 450 страниц в каждой. Хотя эти книги и их разделы подчинены единому плану, всё же, как правило, ими можно пользоваться независимо одна от другой. Более того, разделы этих книг также могут читаться в большой мере независимо друг от друга. В то же время в отдельных статьях книги встречаются ссылки на ту или иную статью «Энциклопедии» [1]). Вот общий план издания:

Книга первая. Арифметика.

Происхождение систем счисления. Понятия множества, группы, кольца и поля; теоретические основы арифметики. Элементы теории чисел. Устный и письменный счёт; вспомогательные средства вычислений.

---

[1]) Ссылки на статьи из той же книги сопровождаются указанием соответствующих страниц; при ссылках на статьи, помещённые в других книгах «Энциклопедии», указывается «См. Э. э. м.» и приводятся номер книги и название статьи.

Книга вторая. Алгебра.

Векторные пространства и линейные преобразования. Кольцо многочленов и поле рациональных функций. Численные и графические методы решения уравнений.

Книга третья. Анализ.

Функции и пределы; рациональная, степенная, показательная и логарифмическая функции; тригонометрические функции и обратные им. Элементы дифференциального и интегрального исчислений. Элементарные функции комплексного переменного.

Книга четвёртая. Геометрия, часть I.

Топологические понятия. Основания геометрии. Понятие о неевклидовых геометриях. Элементы аналитической и проективной геометрии. Геометрические преобразования. Измерение площадей, длин, объёмов и поверхностей.

Книга пятая. Геометрия, часть II.

Многоугольники и многогранники. Круги и сферы. Применения к геодезии и астрономии. Замечательные кривые и поверхности. Задачи на построение. Методы графических изображений.

Книга шестая. Различные вопросы.

Комбинаторика. Элементы теории вероятностей и математической статистики. Знаменитые математические задачи. Математические парадоксы и софизмы. Математические развлечения и игры.

Книга седьмая. Методология и история математики.

Математика и её место среди других наук, основные этапы её развития, методы и задачи. Очерк истории математики. Математика в Советском Союзе. Приложение. Терминологический словарь.

Первая книга открывается статьёй И. Г. Башмаковой и А. П. Юшкевича, посвящённой системам счисления и нумерации, рассматриваемым в культурно-историческом разрезе.

Далее идёт обширная статья И. В. Проскурякова, задача которой заключается в построении теоретических основ арифметики. В двух первых главах статьи рассматриваются весьма общие математические понятия, значение которых далеко выходит за пределы арифметики и которые неоднократно используются как в первой книге, так и в дальнейших. Это понятия множества, группы, кольца и поля.

Центральное место в статье занимает аксиоматическое изложение теории натуральных чисел; это — теоретический фундамент всей арифметики. На основе теории натуральных чисел развёртывается в порядке последовательного обобщения теория целых, рациональных, действительных и, наконец, комплексных чисел. Автор знакомит также с дальнейшими обобщениями понятия числа (гиперкомплексные числа). Вся статья в целом принадлежит к числу наиболее

трудных и отвлечённых во всём настоящем издании; трудности здесь коренятся в самом существе дела. Читатель, не заинтересованный в первую очередь вопросами логического обоснования арифметики, может опустить эту статью, обращаясь по мере надобности для справок к её первым двум главам.

Статья А. Я. Хинчина излагает наиболее элементарные и важные вопросы теории чисел. Сюда относятся вопросы, связанные с теорией делимости, в частности теория цепных (непрерывных) дробей и вопросы приближения иррациональных чисел посредством рациональных.

Наконец, статья В. М. Брадиса посвящена вопросам округления чисел, правилам приближённых вычислений, подсчёта погрешностей и вспомогательным средствам вычислений, включая логарифмическую линейку.

Существенным дополнением к первой книге должны служить сведения об этапах исторического развития понятия числа, о постепенном и весьма длительном формировании общего понятия натурального числа, о развитии понятия дроби, о том прообразе позднейшей теории действительных положительных чисел, который сложился у древних греков (в «Началах Евклида»), о развитии понятия отрицательных и комплексных чисел в связи с теорией уравнений, а впоследствии — аналитической геометрией и анализом. Эти сведения не выделяются нами в отдельную статью; они включаются в общий очерк истории математики, помещаемый в последней книге всего издания.

Редакция

И. Г. БАШМАКОВА и А. П. ЮШКЕВИЧ

ПРОИСХОЖДЕНИЕ СИСТЕМ СЧИСЛЕНИЯ

*

ВВЕДЕНИЕ

Целью всякой нумерации является изображение любого натурального числа с помощью небольшой группы индивидуальных знаков. Этого можно было бы достичь при помощи одного единственного знака 1 (единицы). Каждое натуральное число тогда записывалось бы путём повторения символа единицы столько раз, сколько в этом числе содержится единиц. Сложение свелось бы к простому приписыванию единиц, а вычитание — к их вычёркиванию. Лежащая в основании такой системы идея весьма проста, однако система эта является крайне неудобной. Для записи больших чисел она практически неприменима и ею пользовались только народы, счёт которых не простирался дальше одного-двух десятков.

Наиболее совершенным принципом записи чисел является тот, на котором основана наша десятичная система нумерации. В этой нумерации все числа от 1 до 9 обозначаются индивидуальными символами 1, 2, 3, ..., 9. К ним присоединяется знак 0 для нуля. Любое натуральное число может быть изображено при помощи только этих десяти знаков по принципу поместного или позиционного значения.

Всякое натуральное число n однозначно представимо в виде

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0,$$

где a_i могут принимать значение 0, 1, 2, ..., 9. Тогда число n в позиционной системе запишется так:

$$n = a_m a_{m-1} \ldots a_1 a_0.$$

Каждый символ a_i получает значение, определяемое: 1) его начертанием, 2) его положением в записи числа. Если, например, мы хотим записать четыре тысячи, мы должны поставить цифру 4 на четвёртое место, считая справа; остальные три разряда в данном случае отсутствуют, поэтому на их место ставятся нули: 4000. Таким же образом символ 4 может означать 4 единицы, 4 десятка, 4 сотни и т. д., смотря по тому положению, которое он занимает.

Несмотря на кажущуюся простоту такой системы записи, она явилась продуктом длительного исторического развития, и в создании её принимали участие целые народы. Можно сказать даже, что

создание такой системы является делом всего человечества. Известный французский математик и физик XVIII — XIX вв. Лаплас писал: «Мысль выражать все числа 9 знаками, придавая им, кроме значения по форме, ещё значение по месту, настолько проста, что именно из-за этой простоты трудно понять, насколько она удивительна. Как нелегко было притти к этой мето́де, мы видим на примере величайших гениев греческой учёности Архимеда и Аполлония, от которых эта мысль осталась скрытой».

В качестве основания позиционной системы могут быть взяты и другие числа, отличные от 10. Многие учёные, например, считали, что более удобным основанием было бы число 12, имеющее больше делителей: 2, 3, 4, 6. Особенно широкое распространение десятичной системы связано с количеством пальцев на наших руках. На это обстоятельство впервые обратил внимание Аристотель в своих «Проблемах». Десятичная система на самом деле не обладает какими-либо особыми преимуществами, выделяющими её из позиционных систем с другим основанием. Выбор основания является принципиально произвольным. Разумеется, оно не должно быть слишком большим, так как в этом случае система будет содержать слишком много цифр, очень громоздка будет в ней таблица умножения и т. д. С другой стороны, оно не должно быть и слишком маленьким [1]).

Свидетельством того, что не во все эпохи системы нумерации совпадали с нашей современной, служит уже наша речь. В названиях числительных вовсе не заметно того единообразия, которое имеет место в их записи. Так, в нашем родном языке, кроме различных названий для девяти первых натуральных чисел 1, 2, ..., 9 и нуля, имеется специальное название для десяти (тогда как при письме мы обозначаем десять, как 10, т. е. с помощью 1 и 0). Такие же специальные названия существуют для ряда единиц высших разрядов: сорок [2]), сто, тысяча, миллион и т. д.

Далее, числа, начиная с 11 до 19, мы называем один-на-дцать, ..., девят-на-дцать, т. е. называем некоторое число от 1 до 9 с добавлением «на десять». Частица «на» здесь, очевидно, не означает умножения, и о её происхождении мы скажем ниже.

Числа от 21 до 99 произносятся большею частью по тому же принципу, по которому они записываются: два-дцать один (двадесять один), тридцать два и т. д. Исключениями служат числительные сорок и девяносто [3]). Числа, имеющие индивидуальные, не

---

[1]) Сущность нумерации с произвольным основанием была впервые разобрана Б. Паскалем в сочинении De numeris multiplicibus ex sola characterum numericorum additione agnoscendis («О делимости чисел, выведенной с помощью одного сложения их цифр», 1654, опубл. 1665).

[2]) Число 40 в русской нумерации и у многих народов Востока играло особую роль, о чём будет сказано ниже.

[3]) Слово девяносто не относится к узловым (см. ниже). Есть предположение, что оно возникло как сочетание «девять до ста».

разложимые на составные числительные наименования (один, два, десять, сорок, сто, тысяча, ...), мы будем называть *узловыми*. Числа, наименования которых получаются комбинированием наименований узловых чисел, мы будем называть *алгорифмическими*. Как мы увидим, отличие в наименовании тех и других отражает отличие в их происхождении [1]).

Аналогичные явления имеют место и в других языках. Например, во французском языке сохранились явные остатки двадцатиричной непозиционной системы. Двадцать является тем новым узловым числом, название которого не складывается из названий первых десяти чисел: vingt. Число 80 произносится, как «четыре-двадцать», quatre-vingts, 90 — как «четыре-двадцать-десять», quatre-vingts-dix, 120 — как «шесть-двадцать», six-vingts. В старофранцузском языке, кроме того, 140 произносилось, как «семь-двадцать», 160 — как «восемь-двадцать», 300 — как «пятнадцать-двадцать» и т. д. В романских, немецком, английском языках, как и в русском языке, имеются специальные названия для ста, тысячи и т. д. Следы двадцатиричной системы сохранились, кроме французского, в английском, голландском языках. Так, по-английски слово score означает наряду с иными понятиями число 20, а three score, т. е. «три-двадцать», — шестьдесят. В скандинавских языках сильны, кроме того, следы пятиричной системы.

Таким образом:

1) современная письменная система счисления является строго позиционной, а устная не является строго позиционной;

2) письменная является строго десятичной, устная сохраняет следы существования пятиричной и иных систем;

3) в письменной системе существует только десять узловых чисел 0, 1, 2, ..., 9, в устном счёте имеются и другие узловые числа, каждое из которых служит основанием своей местной системы, т. е. основанием некоторого отрезка числового ряда, а не всего числового ряда (например, в русском языке, начиная от ста, счёт идёт путём комбинирования ста с меньшими узловыми или алгорифмическими числами: сто один, сто два и т. д.).

Можно заметить, что наша устная речь отражает более раннюю стадию счёта, чем наша нумерация. Так, например, римская письменная нумерация, предшествовавшая появлению нашей позиционной системы, родственна по своей структуре устной нумерации современных европейских народов.

---

[1]) Различение «перстов» (числа до 10), «составов» (целых десятков) и «сочинений» (прочие числа в пределах до ста) имеется в «Арифметике» Л. Магницкого (1703). Наиболее ранний известный пример подобного распределения чисел встречается у Герберта в X в. (digiti, articuli, compositi). Очевидно, что мы имеем здесь дело с отражением того же разделения чисел на узловые и алгорифмические. Несомненна также связь терминов «персты» и «суставы» с пальцевым счётом.

Узловыми числами в римской нумерации являются: I — единица, V — пять, X — десять, L — пятьдесят, C — сто, D — пятьсот, M — тысяча. Нуля там нет. Система эта является десятичной непозиционной с сильными следами пятиричной системы (индивидуальные символы для 5, 50, 500). Все алгорифмические числа получаются в результате сложения и вычитания узловых. Например, число 1948 в этой системе запишется так: MCMXLVIII.

Примерно в том же отношении, в каком римская письменная нумерация находится к современному устному счёту, способы счёта многих так называемых «первобытных» народов находились к римской системе нумерации. Уже из сказанного понятно, что для выяснения происхождения систем счисления (как современной позиционной, так и непозиционных) мы должны будем использовать и этнографический и языковедческий материал.

§ 1. Начальная стадия развития счёта

Понятие числа является одним из основных понятий современной математики. Оно является и одним из древнейших понятий. Все культурные народы, обладавшие письменностью, уже имели понятие о числе и те или иные системы счисления. О понятии числа в доисторические времена мы можем судить лишь по косвенным данным. Источником здесь является, во-первых, языкознание, во-вторых, этнография, позволяющая на основании изучения культуры народов, стоящих по классификации Энгельса на стадии дикости и варварства, судить об аналогичных периодах жизни предков современных культурных народов. К сожалению, долгое время собирание этнографического материала составляло монополию миссионеров и колонизаторов. А к концу XIX в., когда ходом развития науки внимание учёных было с особенной силой обращено к доисторическим временам жизни человечества, то оказалось, что так называемых «первобытных» народов почти нет. Империалистическая политика капиталистических стран привела к этому времени к почти поголовному истреблению многих туземных племён. Так, например, австралийское племя тасманийцев к началу XX в. было совершенно уничтожено. То же произошло и с когда-то многочисленным племенем абипонов — обитателей Южной Америки.

При восстановлении стадий развития числа приходится, таким образом, довольствоваться весьма скудным материалом. Однако вопрос о происхождении этого понятия настолько важен, что и та неполная картина, которую удаётся воссоздать, имеет большое значение, в частности для разоблачения существующей буржуазной идеалистической «теории», согласно которой понятие числа и даже всего натурального ряда является у человека врождённым. Известно, например, ходячее изречение Кронекера: «Целые числа создал господь бог, всё остальное — дело рук человеческих». Изучение начальных этапов развития числа и других основных математических понятий полностью опровергает подобные буржуазные «теории». Объективное исследование показывает связь происхождения этих понятий с производственной практикой коллективов первобытных обществ, выясняет, что сама наша «интуиция» не является категорией неизменной и что даже самые, казалось бы, «изначальные»

наши понятия вовсе не являются в действительности врождёнными. Изучение начальных этапов развития числа покажет нам, что и целые числа были созданы людьми, что и они — дело рук человеческих.

Среди буржуазных учёных XIX в. (Тейлор и др.) было также распространено мнение, что «первобытный» человек получал все свои знания о мире путём наблюдения явлений природы, сопоставления с ранее виденным и логических выводов. «Первобытный» человек при этом выступал как некий философ-созерцатель. В действительности человек начал не с теоретизирования, а с труда, с борьбы за существование, не с пассивного наблюдения природы, а с преобразования её.

Маркс в «Замечаниях на книгу А. Вагнера» писал, что отношение человека к природе с самого начала выступает не как теоретическое, а как практическое, т. е. основанное на действии. «Как и всякое животное, они (т. е. люди первобытного общества. — *Авторы*) начинают с того, чтобы *есть, пить* и т. д., т. е. не „стоять" в каком-нибудь отношении, а *активно действовать*, овладевать при помощи действия известными предметами внешнего мира и таким образом удовлетворять свои потребности» [1]).

Труд, — писал Энгельс в «Диалектике природы», — есть «первое основное условие человеческого существования, — и это в такой мере, что мы в известном смысле должны сказать: труд создал самого человека» [2]). Именно в процессе труда были созданы и такие основные понятия, как число, натуральный ряд, фигура, были выработаны простейшие правила счёта и навыки измерения длин, площадей и объёмов.

При этом понятия числа и фигуры и их основные свойства явились отражениями свойств и отношений реальных предметов внешнего мира.

«Понятия числа и фигуры, — писал Энгельс, — заимствованы именно из действительного мира. Десять пальцев, на которых люди учились считать, т. е. производить первое арифметическое действие, представляют что угодно, но только не свободное творение рассудка. Для счёта необходимы не только объекты счёта, но также уже и способность, при рассмотрении этих объектов, отвлекаться от всех их свойств, кроме их числа, а эта способность — продукт долгого исторического эмпирического развития» [3]).

Посмотрим же, каковы были представления о числе и натуральном ряде на первых стадиях культурного развития человечества, и проследим, как, постепенно меняясь и совершенствуясь, они достигли современного уровня.

---

[1]) К. Маркс и Ф. Энгельс, Сочинения, т. XV, стр. 461.
[2]) К. Маркс и Ф. Энгельс, Сочинения, т. XIV, стр. 452.
[3]) К. Маркс и Ф. Энгельс, Сочинения, т. XIV, стр. 39.

К сожалению, материалы, имеющиеся в нашем распоряжении, не позволяют достаточно определённо связать различные этапы развития счёта с данной Энгельсом в работе «Происхождение семьи, частной собственности и государства» периодизацией доисторических ступеней культуры.

Ещё и в наше время известны народы, в языке которых имеются только два числительных: один и два. У многих племён Австралии и Полинезии в самое недавнее время этим дело и ограничивалось. При помощи сочетания названных числительных эти племена образуют числа 3 = два-один, 4 = два-два, 5 = два-два-один, 6 = два-два-два. Так, например, у западных племён островов Торресова пролива единственными числительными являются 1 — урапун и 2 — окоза. Далее они считают 3 = окоза-урапун, 4 = окоза-окоза, 5 = = окоза-окоза-урапун, 6 = окоза-окоза-окоза. Этот способ счёта положил начало древнейшей из всех систем счисления — двоичной системе [1]). Следы её мы находим неоднократно в египетском способе умножения и деления, в системе египетских дробей [2]), в том, что во многих языках, например в старославянском, наряду с единственным и множественным числами имеется и двойственное число [3]).

[1]) Для устной и письменной нумерации двоичная система неудобна, так как запись чисел в ней слишком длинна (например, число 777 в ней запишется 1 100 001 001), но она имеет и существенные преимущества.

На принципиальные достоинства двоичной системы первый обратил внимание Лейбниц, отмечавший особую простоту операций в ней (таблицы сложения и умножения сводятся к $1 + 1 = 10$, $1 \cdot 1 = 1$; при делении не нужны догадки и пробы). Лейбниц не рекомендовал эту систему взамен десятичной для практического счёта, но подчёркивал, что «вычисление с помощью двоек, т. е. 0 и 1, в вознаграждение его длиннот, является для науки основным и порождает новые открытия, которые оказываются полезными впоследствии, даже в практике чисел, а особенно в геометрии: причиной чего служит то обстоятельство, что при сведении чисел к простейшим началам, каковы 0 и 1, всюду выявляется чудесный порядок» (в Explication de l'arithmétique binaire, qui se sert des seuls caractères 0 et 1, avec des remarques sur son utilité, 1703 в Leibnizens mathematische Schriften, hsg. v. C. I. Gerhardt, т. VII, Halle, 1863, стр. 225; ср. там же письма Лейбница к Шуленбургу от 1698 г.). Действительно, двоичная система оказалась весьма удобной в ряде теоретических исследований.

Лейбниц, однако, не предвидел, что двоичная система принесёт пользу в вычислительной математике, — именно будет положена в основу устройства электронных счётных машин, как это произошло в последнее время. Производство вычислений на таких машинах с избытком компенсирует затрату труда на переход от десятичной системы к двоичной в начале операций и обратный переход в окончательном результате. См. Л. Д. Кудрявцев, О принципах производства арифметических операций на вычислительных машинах. Успехи математических наук, т. V, вып. 3 (1950).

[2]) См. в параграфе, посвящённом дробям, о роли половинного ряда в старинных русских дробях.

[3]) В некоторых языках существовало и тройственное число как пережиток троичной системы. На особую древность первых трёх числительных указывает и то обстоятельство, что во многих языках они в отличие от остальных числительных изменяются по родам (один, одна, одно; два, две; лат. tres, tria).

О числах выше 6 островитяне Торресова пролива говорят «много-много», «множество» или «неисчислимо» [1]). У некоторых племён слова «много», «неисчислимо» применяются для обозначения всех чисел $\geqslant 3$.

Таким образом, на этой стадии натуральный ряд является конечным и состоит подчас только из двух членов.

Но не следует думать, что племена, у которых существуют числительные только для единицы и для двух, не умеют сосчитывать совокупности, состоящие более чем из двух или шести предметов. Человек научился в известном смысле «считать» задолго до того, как появились названия чисел. Один из наблюдателей пишет об абипонах, у которых существовали лишь числительные один, два и три, что, сбираясь на охоту, они, сидя уже в седле, осматриваются вокруг, и если нехватает хотя бы одной из многочисленных собак, которых они содержат, то они принимаются звать её. Наблюдателя особенно удивило, каким образом, не умея считать, абипоны способны были сейчас же сказать, что среди такой значительной своры нехватает одной собаки.

Дело в том, что на этой стадии численность воспринимается как одно из свойств совокупности предметов, характеризующее эту совокупность наряду с другими свойствами: цветом, формой, размером и т. д. А именно, это свойство характеризует совокупность, во-первых, со стороны её целостности (все ли предметы данной совокупности имеются налицо), а во-вторых, в чисто порядковом соотношении с другими совокупностями, составленными из тех же предметов (больше или меньше одна совокупность, чем другие).

Очевидно, такой «счёт» был достаточен только на той стадии развития человечества, когда, грубо говоря, нечего было считать, когда ещё хозяйство племени стояло на очень низком уровне, а межплеменные связи не были налажены.

Итак, на первой стадии развития числа оно представляет собой отдельные числа-свойства или числа-качества конкретных совокупностей предметов с едва намечающимися порядковыми соотношениями.

В настоящее время уже не известны народы, счёт которых остановился бы на этой первой стадии, соответствующей в основном первой и второй ступеням дикости. «Счёт» числами-свойствами сохранился у некоторых племён только в качестве пережитка.

---

[1]) Следы того, что число 7 служило одновременно для обозначения неопределённой множественности и у наших предков, сохранились в русском языке в виде пословиц и поговорок, например: «Семеро одного не ждут», «Семь раз отмерь, один раз отрежь», «У семи нянек дитя без глаза» и т. д. Во всех этих пословицах слово «семь», очевидно, употребляется в смысле «много».

С изобретением лука и стрел, с переходом к систематическим охотам, с расселением деревнями и налаживанием связей, сначала — между отдельными деревнями, а затем и между племенами, короче — с переходом к высшей ступени дикости старый «счёт» числами-свойствами оказался уже недостаточным. Нужно было уже не только уметь определять «на-глаз» численность некоторой совокупности, но и уметь сообщать о её численности. Например, нужно было передать нескольким племенам, что через определённое количество новолуний назначается сбор для переговоров или совместной охоты, или передать, чтобы все союзные племена через определённый срок выставили бы некоторое число воинов. Для этого арунта (австралийцы) и полинезийцы пользуются следующим способом: когда число, подлежащее счёту, оказывается большим, туземцы прибегают к помощи различных частей тела, из которых каждая имеет своё название и своё точно обусловленное место в этой системе счисления. Определённое число перечисленных таким образом частей тела, начиная с мизинца одной из рук, означает такое же число воинов, дней или месяцев, судя по обстоятельствам.

Счёт обычно начинается с мизинца левой руки, перебираются все пальцы, затем переходят к запястью, локтю, плечу и т. д. до мизинца правой руки, после чего, если совокупность ещё не исчерпана, идут в обратном порядке. В деловых отношениях туземцу достаточно вспомнить, до какой части своего тела он дошёл при подсчёте предметов и, воспроизведя счёт, начиная со своего левого мизинца, вновь найти искомое число.

У островитян Торресова пролива на человеческом теле изображаются таким образом числа до 33. Если пересчитываемая совокупность имеет более 33 членов, то они прибегают к пучку палочек. Именно то обстоятельство, что при исчерпании всех частей тела, каждая из которых индивидуализирована, люди прибегают к пучку палочек (причём все палочки пучка примерно одинаковы), даёт нам ключ к пониманию первоначального назначения такой «живой» шкалы. Ясно, что сначала она была нужна не для индивидуализации чисел, а лишь для установления равночисленности двух совокупностей, или, иначе, для установления взаимно однозначного соответствия между предметами обеих этих совокупностей.

Пережитки такого способа счёта сохранились у многих племён, стоявших на более высокой стадии развития. Так, некоторые из них для тех же целей пользовались верёвкой с узелками, другие — чётками или просто бирками (деревянные палочки с зарубками). Племена Перу вели запись чисел при помощи верёвок с узелками (так называемое квипу, рис. 1). Верёвки связывались по четыре вместе и к ним присоединялась пятая верёвка, на которой при помощи узлов выражалось число, являющееся суммой чисел на первых четырёх верёвках. Узлы, обозначающие единицы, десятки и

Рис. 1

сотни в данном числе, были различной формы. В период владычества инков (XI—XVI вв. н. э.) при помощи таких квипу «записывались» настоящие бухгалтерские отчёты. Такие верёвки с узелками служили только для записи чисел [1]). Для производства арифметических операций употреблялись камешки или зёрна маиса.

Однако число на этой стадии не воспринималось как то́ общее, что имеют между собой все равночисленные совокупности. Тогда просто удовлетворялись констатированием равночисленности.

В тех случаях, когда сосчитываемая совокупность содержала небольшое количество предметов ($\leqslant 20$), обычно выбиралась некоторая определённая совокупность из множества совокупностей, имеющих одинаковое число предметов, и про остальные совокупности этого множества говорили, что в них столько же предметов, сколько в этой выбранной. Например, чтобы выразить, что в некоторой совокупности пять предметов, говорили, что в ней столько же предметов, сколько пальцев на руке. Общее свойство всех равночисленных конечных множеств — число — выражалось через свойство «особенного» множества, некоторого выбранного частного множества из этой совокупности. Интересно, что у племён, стоящих на отмеченной стадии развития, применяется тот же приём для образования и других понятий. Так, у тасманийцев не было слов для обозначения общих понятий вроде твёрдый, горячий, холодный, круглый и т. д. Для обозначения твёрдости они говорили «как камень», чтобы выразить, что предмет круглый, говорили «как луна» или «как шар». То же имело место и для обозначения цветов. На этой стадии нет и таких общих понятий, как дерево или рыба, но существуют отдельные слова для обозначения каждого вида рыб или деревьев.

Итак, эта фаза в истории возникновения отвлечённых чисел характеризуется изображением сосчитываемых множеств при помощи частей тела, особенно пальцев рук и ног, палочек, узлов верёвки и т. д. Несмотря на крайнюю примитивность этого способа изображения, он сыграл исключительную роль в развитии понятия числа. Действительно, существенной стороной этого приёма является то, что в нём мы имеем способ изображения всех

---

[1]) Геродот следующим образом описывает распоряжение Дария, данное им ионийцам после переправы через реку Истр во время предпринятого им похода на скифов (VI в. до н. э.): «После этого царь завязал на ремне шестьдесят узлов, позвал на совещание всех ионийских тиранов и сказал им: „прежде высказанное мною решение относительно моста, ионийцы, я отменяю; теперь возьмите этот ремень и поступите так: начиная как раз с того времени, когда я пойду на скифов, развязывайте на ремне каждый день по одному узлу; если бы за этот промежуток времени я не явился бы назад и миновало бы число дней, обозначенное узлами, плывите обратно на родину; а до той поры оберегайте мост, приложите всяческое старание к защите его и сохранению в целости“».

исчисляемых множеств при помощи одной определённой системы, приведённой с ними в соответствие.

Такой способ счёта при своём дальнейшем развитии привёл к созданию пятиричной, десятичной и двадцатиричной систем счисления. Например, жители Миралуги (остров в Торресовом проливе) говорят: 5 = набигет, 10 = набигет, набигет, 15 = набикоку, 20 = набикоку, набигет. Гет означает руку, коку — ногу. При этом наблюдатель добавляет: «Не следует думать, что набигет является именем числительным 5, оно выражает только, что дело идёт о стольких же предметах, сколько на руке пальцев».

По сообщению нашего замечательного учёного-путешественника Н. Н. Миклухи-Маклая туземцы новой Гвинеи считают следующим образом: «Излюбленный способ счёта состоит в том, что папуас загибает один за другим пальцы руки, причём издаёт определённый звук, например, „бе, бе, бе“... Досчитав до пяти, он говорит „ибон-бе“ (рука). Затем он загибает пальцы другой руки, снова повторяет „бе, бе“..., пока не доходит до „ибон-али“ (две руки). Затем он идёт дальше, приговаривая „бе, бе“..., пока не доходит до „самба-бе“ и „самба-али“ (одна нога, две ноги). Если нужно считать дальше, папуас пользуется пальцами рук и ног кого-нибудь другого» [1]).

Аналогичные наименования числительных зарегистрированы и у многих других племён. С этой стадией развития числа и счёта связан получивший широкое распространение счёт на пальцах (так называемый инструментальный счёт). С пальцевым счётом, как говорилось, связано было и деление на «персты» и «суставы».

Все вышеописанные стадии развития числа можно отнести ориентировочно к периоду дикости.

С дальнейшим развитием общества всё больший круг совокупностей попадает в число сосчитываемых. Простое установление равночисленности и ручной счёт уже не могут удовлетворять новых потребностей коллектива; хотя ручной способ счёта в качестве пережитка сохраняется ещё долгое время [2]), но основная линия развития, приведшая к созданию натуральных чисел, пошла в другом направлении. Появившаяся новая система счёта может быть названа групповой или иначе счётом при помощи чисел-совокупностей.

Зародыши такого счёта имелись и на более ранних ступенях развития. Так, наблюдатели отмечают у островитян западной части

---

[1]) Н. Миклухо-Маклай, Путешествия, Изд. АН СССР, 1940, т. I, стр. 280.

[2]) Ещё в 1529 г. в Базеле вышла написанная задолго до того книга Беды Достопочтенного (672—735), в которой излагаются способы счёта на пальцах, причём счёт этот распространяется на все числа вплоть до миллиона. Сравнительно до недавнего времени счётом на пальцах пользовались китайские и монгольские купцы.

Торресова пролива «отчётливо выраженную склонность считать группами по два, попарно». То же самое отмечает другой наблюдатель относительно счёта на острове принца Йоркского. При этом счёт одних предметов ведётся по преимуществу парами, других — десятками или сотнями и т. д. Таким образом, при счёте определённого вида предметов предметы эти всегда соединяются в определённые, устойчивые группы. В качестве пережитка такого счёта упомянем счёт дюжинами, вплоть до наших дней сохраняющийся в Европе для некоторых групп вещей (рубашки, стулья, посуда, карандаши, резинки, перья). При этом дюжина образовывала единицу счёта, дюжина дюжин составляла гросс, а дюжина гроссов — массу [1]). Особенное распространение такой счёт имел у племён, стоявших на первых двух ступенях варварства. Постепенно каждая такая устойчивая группа получала название, которое выражало как вид сосчитываемых предметов, так и их число. Такого рода группы, с помощью которых вёлся счёт, мы и будем называть *числами-совокупностями.*

На островах Фиджи и Соломоновых существуют собирательные имена, обозначающие десятки произвольно подобранных вещей: ни числа в отдельности, ни названия предметов они не выражают. На Фиджи имеются также названия для 100 челноков, 100 кокосовых орехов, для 1000 кокосовых орехов и т. п. Если две такие группы равночисленны, то это обычно отображается в названии соответствующих чисел-совокупностей. Так, у туземцев Флориды на-куа означает 10 яиц, на-банара — 10 корзин с продовольствием, но отдельно слово «на», которое соответствовало бы числу 10, не употребляется. На одном из диалектов индейцев Западной Канады слово «тха» означает 3 вещи, тхане — 3 лица, тхат — 3 раза, тхатоэн — в трёх местах и т. д. Но слова, которое бы обозначало отвлечённое число три, там нет. Однако наличие в названиях всех равночисленных совокупностей одной и той же частицы показывает, что на этой стадии уже начинают констатировать, что все такие группы имеют нечто общее, именно, одну и ту же численность. На этой стадии развития не всякой группе предметов приписывается число, только те группы являются числами-совокупностями, которые часто встречаются в хозяйственном или ином обиходе племени. Если в VI в. до н. э. пифагорейцы объявили, что «всё есть число», то можно сказать, что на рассматриваемой стадии развития не всё было числом.

Числа на этой стадии были именованными по существу, отвлечённых чисел ещё не существовало. Постепенно устойчивые числа-совокупности начинают рассматриваться как новые единицы, которыми и ведётся счёт. Уже в этом взгляде на некоторую совокуп-

---

[1]) Двенадцатиричная система встречается и ныне у некоторых племён в Судане.

ность предметов как на новую единицу счёта заключена возможность создания системы счисления.

Со временем такими устойчивыми числами-совокупностями стали считать не только данные предметы, для которых эти числа были установлены, но и предметы, сходные с ними по форме или по употреблению. Таким образом, в некоторых первобытных языках образовалось несколько рядов числительных. Так, в языке чимшиенов (Британская Колумбия) имеется семь различных рядов чисел, употребляющихся для счёта 1) неопределённых предметов, 2) плоских предметов, 3) круглых предметов и деления времени, 4) людей, 5) длинных предметов (числа при этом комбинируются со словом дерево), 6) лодок, 7) мер. Пережитки счёта числами-совокупностями наблюдались ещё в Древней Греции. Так, Аристотель в «Метафизике» обсуждает вопрос о том, одинаковы ли единицы в одном и том же числе и являются ли они одинаковыми или различными в разных числах. Ещё Диофант (III в. н. э.) после цифр, выражающих некоторое число, всегда ставил М — первую букву слова μονας — единица, т. е. записывал число некоторых одинаковых между собой единиц.

Под влиянием обмена один из рядов чисел начал вытеснять все другие. Это был тот числовой ряд, который служил для счёта денег (ими на первых порах являлись раковины или скот). Имена числительные, — как сообщает один наблюдатель, — представляются уму йорубов (йорубы — племя Центральной Африки) одновременно в двух значениях: во-первых, как число, во-вторых, как та вещь, которую йорубы преимущественно пересчитывают, т. е. «каури» — раковины, играющие у йорубов роль монет. Так возникали универсальные числа, т. е. такие, с помощью которых можно считать любые предметы.

Однако числа-совокупности явились прообразами только наших узловых чисел. Если счёт вёлся десятками, двадцатками или дюжинами некоторых предметов, то описанным только что образом не могли возникнуть, например, числа 17 и 19, т. е. алгорифмические числа. Более того, если бы все числа возникали по описанной схеме, то они существовали бы как не связанные между собой понятия, и количественные отношения между ними были бы совершенно неясны. Мы покажем далее, что алгорифмические числа возникли путём комбинаций узловых чисел как результат о п е р а ц и й, производимых над узловыми числами.

При изучении языка кламатов, индейцев Северной Америки, а также племён Британской Колумбии оказалось, что при счёте ими употребляются специальные глаголы, названные исследователями глаголами-классификаторами. Эти глаголы служат для характеристики определённого способа размещения. Если число предметов устойчивой группы, с помощью которой ведётся счёт, равно 10, то первые 10 чисел не сопровождаются этими глаголами. Этот факт

исследователи объясняют особенностями счёта у индейцев. 10 первых сосчитываемых предметов они складывают на землю в стопку или в ряд, а с одиннадцатого предмета начинается новая стопка или ряд. Глаголы-классификаторы не сопровождают также чисел, кратных десяти. Таким образом, эти термины служат только для того, чтобы размещать по разрядам единицу или единицы, следующие за десятками, а не самые десятки. Так, чтобы выразить наличие 26 предметов, индеец должен был сказать: «на дважды десять плодов (или других предметов) я кладу сверху шесть». Таким образом, алгорифмические числа сразу же появляются как результат некоторых операций над узловыми числами. Операции эти вначале были, однако, не арифметическими, а двигательными. Следы этого сохранились во многих языках. Так, у нас в русском языке числительные от 10 до 19 произносятся, как соответствующее число единиц «на-десять»: двенадцать (два-на-десять), пятнадцать (пять-на-десять) и т. д. Здесь частичку «на», повидимому, следует понимать именно в смысле «положить на».

Хорошей иллюстрацией к способу счёта при помощи определённого расположения предметов могут служить числовые обозначения ацтеков [1]) в XV—XVI вв. Так у ацтеков число 6 обозначалось , 7 — и т. д. Очевидно, основная группа состояла здесь из пяти предметов. Черта отделяла одну такую группу от следующей. Сама черта числового значения не имела.

Впоследствии непосредственно двигательный характер операций всё более и более утрачивается, и всё более и более выступает арифметический их смысл. Например, в угро-финских языках число 8 определяется как разность между узловым числом 10 и узловым числом 2. Произносится 8 на этих языках, как «два-десять», 80— как «два, сто» и 800 — как «два, десять, сто» (здесь «десять, сто» является обозначением для тысячи).

На этой стадии числовой ряд ещё не мыслится однородным. Узловые числа существуют в нём как некие индивидуальные островки, от которых в ту и в другую стороны располагаются алгорифмические числа. Основную роль в их образовании играет операция сложения, однако наряду с ней принимают участие вычитание и умножение. Так, упомянутые выше йорубы имеют следующую систему чисел:

$$11 = 10 + 1,\ 12 = 10 + 2,\ \ldots,\ 15 = 10 + 5,$$
$$16 = 20 - 4,\ 17 = 20 - 3,\ \ldots,\ 19 = 20 - 1.$$

Число 20 является новым узловым; с его помощью образуются дальнейшие числа, причём в их образовании принимают участие как

[1]) Индийское племя, проживающее в Мексике.

сложение и вычитание, так и умножение. Число 70 в этой системе получается, как $20 \cdot 4 - 10$, $190 -$ как $20 \cdot 10 - 10$. Аналогичные приёмы сохранились в римской нумерации. Например, число XVIII читалось по-латыни: duo de viginti, т. е. 2 из 20.

Но числовой ряд на этой стадии не только не является однородным, он не является и неограниченным. С развитием понятия числа он сначала лишь всё более удлиняется. При этом слова «много», «неисчислимо», которые употреблялись раньше для обозначения всех чисел $\geqslant 3$ или $\geqslant 10$, отодвигаются всё дальше, обозначая числа $\geqslant 100$, $\geqslant 1000$ и т. д. [1]). Следующий шаг заключается в том, что это слово, означающее первоначально неопределённое множество, становится названием чисел 100 или 1000 в зависимости от развитости системы счисления данного народа. Так, например, одно и то же слово означает 3 на острове Менгоне, 10 — на острове Фиджи и 10 000 у маорийцев. Маорийцы и народы названных островов имеют примерно одинаковый язык, хотя и стоят на различных ступенях развития культуры.

Натуральный ряд не мыслился бесконечным ещё долгое время. Из предисловия к «Исчислению песка» Архимеда видно, что даже грекам в III в. до н. э. ещё не было очевидно, что можно выразить сколь угодно большие числа, например бóльшие, чем число песчинок в сфере радиуса, равного расстоянию от Солнца до неподвижных звёзд. Основная цель сочинения Архимеда заключалась именно в создании систематического приёма построения и словесного обозначения сколь угодно больших чисел.

---

[1]) Одним из ярких примеров такого рода предельных чисел является число 40, которое служило в русском счёте для обозначения неопределённо большого множества. На такую роль этого числа указывает как его индивидуальное название, так и сохранившееся в качестве пережитка употребление его для обозначения неопределённо большого количества предметов — сорок сороков церквей, сорок сороков чёрных соболей. На ту же роль числа 40 указывает ряд связанных с ним религиозных обычаев и народных поверий: например, сороковой медведь считался последним в жизни охотника

«сорок медведей он взял на рогатину, на сорок первом сплошал»

(Н. А. Некрасов).

В более позднее время, когда число 40 перестало уже быть «предельным», оно стало играть большую роль в русской метрологии в качестве основания системы мер: пуд содержал 40 фунтов, бочка-сороковка — 40 вёдер и т. д.

Сорок играло роль предельного числа и у многих народов Ближнего Востока. Это нашло отражение, например, в знаменитом армянском эпосе «Давид Сасунский»:

«Спустился в яму Мсра-Мелик.
Вот сорок буйволовых шкур взвалили на него,
Огромных сорок жерновов взвалили на него...».

Кончается эпос поминанием всех его героев:

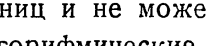
«Великих праотцев наших — сорок раз помянем добром.
Санасара и брата его Богдасара — помянем добром.
Мгера старшего сорок раз помянем добром».

§ 2. Непозиционные системы счисления

К моменту возникновения письменности строение числового ряда представлялось примерно так: узловые числа, существовавшие как некие индивидуальные понятия, принимались каждое за основание своей, местной системы счисления. Наименьшее из узловых чисел принималось за основание первой системы. Далее, счёт шёл путём прибавления единиц к этому узловому числу, а также путём удвоения, утроения и т. д. этого числа, т. е. путём образования алгорифмических чисел, до тех пор пока не достигалось следующее узловое число. После этого начиналась следующая местная система счисления, основанием которой служило это второе узловое число, а алгорифмические числа этой второй системы составлялись путём комбинаций второго узлового числа с первым. Такие алгорифмические числа шли до следующего узлового числа, которое служило основанием третьей местной системы счисления и т. д. [1]).

Схема эта могла быть несколько иной: например, алгорифмические числа могли располагаться по обе стороны от каждого узлового числа, получаясь из него как путём сложения, так и путём вычитания меньших узловых чисел.

При записи чисел, образованных по первой схеме, получались системы типа египетской иероглифической (табл. 1). Узловыми числами здесь являлись единица , десять , сто и тысяча [2]), причём символ для тысячи означал первоначально неопределённое множество.

Эта запись отражает представление о каждом узловом числе как о новой индивидуальности. Из способа записи не видно, что каждое последующее узловое число получается из предыдущего умножением на десять. Все узловые числа имеют абсолютный характер; означает 10 единиц и не может означать, например, 10 десятков или 10 сотен. Алгорифмические числа в египетской системе получаются вполне единообразно при помощи единственной арифметической операции — сложения. Например, число 333 записывается в этой системе так:  .

---

[1]) Читатель, знакомый с канторовской теорией трансфинитов, легко заметит сходство подобного способа образования натурального ряда со способом, употреблённым Кантором. Действительно, Кантор вводит два принципа образования трансфинитов: 1) взятие кратного и прибавление единицы, 2) введение нового индивидуального числа, рассматриваемого как предел предшествующих. Разница та, что в натуральном ряде это новое число уже дано и всегда достижимо — это просто следующее узловое число.

[2]) Полагают, что иероглиф являлся изображением мерительной верёвки, делившейся на 100 частей, а иероглиф для тысячи — изображением цветка лотоса.

Числовые знаки разных народов

	Египетские			Ассиро-Вавилонские	Финикийские	Сирийские	Пальмирские	Греческие Геродиановы	Римские
	Иероглифы 1	Иератические 2	Демотические 3	4	5	6	7	8	9
1	𓏺	𓏺	𓏺	𒁹	𐤀	𐡀	𐡀	Ι	I
2	𓏺𓏺	𓏺𓏺	𓏺𓏺	𒁹𒁹	𐤀𐤀	𐡀𐡀	𐡀𐡀	ΙΙ	II
3	𓏺𓏺𓏺	𓏺𓏺𓏺	𓏺𓏺𓏺	𒁹𒁹𒁹	𐤀𐤀𐤀	𐡀𐡀𐡀	𐡀𐡀𐡀	ΙΙΙ	III
4	𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺	𒁹𒁹𒁹𒁹	𐤀𐤀𐤀𐤀	𐡀𐡀𐡀𐡀	𐡀𐡀𐡀𐡀	ΙΙΙΙ	IV
5	𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺	𒁹𒁹𒁹𒁹𒁹	𐤀𐤀𐤀𐤀𐤀	𐡀𐡀𐡀𐡀𐡀	𐡀𐡀𐡀𐡀𐡀	Γ	V
6	𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺	𒁹𒁹𒁹𒁹𒁹𒁹	𐤀𐤀𐤀𐤀𐤀𐤀	𐡀𐡀𐡀𐡀𐡀𐡀	𐡀𐡀𐡀𐡀𐡀𐡀	ΓΙ	VI
7	𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𒁹𒁹𒁹𒁹𒁹𒁹𒁹	𐤀𐤀𐤀𐤀𐤀𐤀𐤀	𐡀𐡀𐡀𐡀𐡀𐡀𐡀	𐡀𐡀𐡀𐡀𐡀𐡀𐡀	ΓΙΙ	VII
8	𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹	𐤀𐤀𐤀𐤀𐤀𐤀𐤀𐤀	𐡀𐡀𐡀𐡀𐡀𐡀𐡀𐡀	𐡀𐡀𐡀𐡀𐡀𐡀𐡀𐡀	ΓΙΙΙ	VIII
9	𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺𓏺	𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹	𐤀𐤀𐤀𐤀𐤀𐤀𐤀𐤀𐤀	𐡀𐡀𐡀𐡀𐡀𐡀𐡀𐡀𐡀	𐡀𐡀𐡀𐡀𐡀𐡀𐡀𐡀𐡀	ΓΙΙΙΙ	IX
10	𓎆	𓎆	𓎆	𒌋	𐤊	𐡊	𐡊	Δ	X
11	𓎆𓏺	𓎆𓏺	𓎆𓏺	𒌋𒁹	𐤊𐤀	𐡊𐡀	𐡊𐡀	ΔΙ	XI
15	𓎆𓏺𓏺𓏺	𓎆𓏺	𓎆𓏺	𒌋𒁹𒁹𒁹	𐤊𐤀𐤀𐤀	𐡊𐡀𐡀𐡀	𐡊𐡀𐡀𐡀	ΔΓ	XV
20	𓎆𓎆	𓎆	𓎆	𒌋𒌋	𐤊	𐡊	𐡊	ΔΔ	XX
30	𓎆𓎆𓎆	𓎆	𓎆	𒌋𒌋𒌋	𐤊𐤊	𐡊𐡊	𐡊𐡊	ΔΔΔ	XXX
40	𓎆𓎆𓎆𓎆	𓎆	𓎆	𒌋𒌋𒌋𒌋	𐤊𐤊	𐡊𐡊	𐡊𐡊	ΔΔΔΔ	XL
50	𓎆𓎆𓎆𓎆𓎆	𓎆	𓎆	𒌋𒌋𒌋𒌋𒌋	𐤊𐤊𐤊	𐡊𐡊𐡊	𐡊𐡊𐡊	Ⓟ	L
60	𓎆𓎆𓎆𓎆𓎆𓎆	𓎆	𓎆	𒌋	𐤊𐤊𐤊	𐡊𐡊𐡊	𐡊𐡊𐡊	ⓅΔ	LX
70	𓎆𓎆𓎆𓎆𓎆𓎆𓎆	𓎆	𓎆	𒌋𒁹	𐤊𐤊𐤊𐤊	𐡊𐡊𐡊𐡊	𐡊𐡊𐡊𐡊	ⓅΔΔ	LXX
80	𓎆𓎆𓎆𓎆𓎆𓎆𓎆𓎆	𓎆	𓎆	𒌋𒁹𒁹	𐤊𐤊𐤊𐤊𐤊	𐡊𐡊𐡊𐡊𐡊	𐡊𐡊𐡊𐡊𐡊	ⓅΔΔΔ	LXXX
90	𓎆𓎆𓎆𓎆𓎆𓎆𓎆𓎆𓎆	𓎆	𓎆	𒌋𒁹𒁹𒁹	𐤊𐤊𐤊𐤊𐤊𐤊	𐡊𐡊𐡊𐡊𐡊𐡊	𐡊𐡊𐡊𐡊𐡊𐡊	ⓅΔΔΔΔ	XC
100	𓍢	𓍢	𓍢	𒌋	𐤑	𐡑	𐡑	Η	C
200	𓍢𓍢	𓍢	𓍢	𒌋𒌋	𐤑𐤑	𐡑𐡑	𐡑𐡑	ΗΗ	CC
400	𓍢𓍢𓍢𓍢	𓍢	𓍢	𒌋𒌋𒌋𒌋			𐡑𐡑𐡑𐡑	ΗΗΗΗ	CD
500	𓍢𓍢𓍢𓍢𓍢	𓍢	𓍢	𒌋𒌋𒌋𒌋𒌋			𐡑𐡑𐡑𐡑𐡑	Ⓟ	D
1000	𓆼	𓆼	𓆼	𒐼			𐡌	Χ	M
10000	𓂭			𒐼𒌋				Μ	
10^5	𓁨								
10^6	𓁩								
10^7	𓁪								

Египетская система интересна ещё по той роли, которую там играет число два. Повидимому, оно служило первоначально основанием системы счисления. Три было уже символом неопределённой множественности. Это видно из того, что для выражения множественного числа некоторого предмета или понятия египтяне под знаком соответствующего иероглифа ставили три чёрточки.

Пережитки двоичной системы отразились в способе умножения египтян, которое они производили путём последовательного удвоения и сложения. Например, для умножения некоторого числа n на 15 египтяне поступали (схематически) так:

$$n \cdot 15 = n(1 + 2 + 2^2 + 2^3) = n \cdot 1 + n \cdot 2 + n \cdot 2^2 + n \cdot 2^3,$$

т. е. они представляли множитель по двоичной системе, а затем умножение производилось отдельно на каждый двоичный разряд. Следы двоичной системы носят на себе и египетские дроби, о чём будет сказано ниже.

Системами типа египетской иероглифической являются финикийская, сирийская, пальмирская, критская, греческая геродианова или аттическая (см. табл. 1).

Аттическая или геродианова нумерация [1]), как показывает само её название, возникла в Аттике. Древнейшая запись по этой системе относится к VI в. до н. э. Числовым знаком для единицы здесь, как и в Египте, является вертикальная черта, повторение которой образует знаки чисел до 4. Число 5 обозначается символом Γ, 10 — Δ, 100 — Η, 1000 — Χ, 10 000 — Μ. Как теперь установлено (впервые на это обратил внимание ещё в XVII в. Валлис), символы эти являются первыми буквами названий соответствующих чисел. Действительно, пять по-гречески будет πέντε (в аттических областях Γ служила для обозначения буквы Π, поэтому писалось ΓΕΝΤΕ), десять — ΔΕΚΑ, сто — ΗΕΚΑΤΟΝ, тысяча — ΧΙΛΙΟΙ и десять тысяч — ΜΥΡΙΟΙ. Числа 50, 500 и 5000 записывались путём комбинирования знака для пяти со знаками для десяти, ста и тысячи: $\Gamma^{\Delta} = 50$, $\Gamma^{H} = 500$, $\Gamma^{X} = 5000$. Остальные числа записывались по аддитивному принципу. Так, число 325 записывалось, как ΗΗΗΔΔΓ. Эта нумерация продержалась в Аттике вплоть до I в. н. э., хотя в других греческих землях она была задолго до того вытеснена более удобной ионийской системой нумерации.

Второй схеме образования натуральных чисел соответствует римская система нумерации. Подобного же типа (с применением вычитания), как мы видели, была и система йорубов. Конечно, римляне не стояли на той же стадии развития, что и йорубы. Римская

[1]) Геродиан — греческий историк II—III в. н. э., из произведений которого западноевропейские учёные впервые узнали об аттической нумерации.

Таблица 2

Числовые знаки разных народов

	Китайские			Цифры Карошти	Цифры пещерной надписи Назик	Цифры ацтеков	Цифры племени Маия
	Старые 1	Коммерческие 2	Научные 3	4	5	6	7
0		○	○				
1	一	丨	丨	丨	—	·	•
2	二	丨丨	丨丨	丨丨	=	··	••
3	三	丨丨丨	丨丨丨	丨丨丨	≡	∴	•••
4	四	乂	丨丨丨丨	×	𐤀;𐤀	::	••••
5	五	𐤄	丨丨丨丨丨	丨×	𐤀;𐤀	⁝⁝	—
6	六	亠	丅	丨丨×	𐤄	⁝⁝|·	·̇
7	七	亠	丌		𐤄	⁝⁝|··	·̇·
8	八	亖	丌丌	××	𐤄;𐤄	⁝⁝|∴	·̇··
9	九	𐤄	丌丌丌		𐤄	⁝⁝|::	·̇··
10	十	十	丨○	𐤄	𐤄;𐤄	◇	═
15	十五	十𐤄	丨≣			◇⁝⁝	≡
20	二十	丨丨十	丨丨○	𐤄	𐤀	𐤐	
30	三十	丨丨丨十	丨丨丨○			𐤐◇	
40	四十	乂十	丨丨丨丨○		𐤀	𐤐𐤐	
50	五十	𐤄十	丨丨丨丨丨○	𐤄𐤄𐤄		𐤐𐤐◇	
60	六十	亠十	丅○	𐤄𐤄𐤄		𐤐𐤐𐤐	
70	七十	亠十	丌○	𐤄𐤄𐤄𐤄	𐤀	𐤐𐤐𐤐◇	
80	八十	亖十	丌丌○			𐤐𐤐𐤐𐤐	
90	九十	𐤄十	丌丌丌○			𐤐𐤐𐤐𐤐◇	
100	百	𐤇	丨○○	人丨	𐤌	𐤍	
200	二百	丨丨𐤇	丨丨○○	𐤍丨丨	𐤌	𐤍	
400	四百	乂𐤇	丨丨丨丨○○			𐤍	
500	五百	𐤄𐤇	丨丨丨丨丨○○		𐤌	𐤍𐤍	
1000	千	千	丨○○○		𐤍	𐤍𐤍𐤍	
8000	八千	亖千	丌丌○○○		𐤍𐤍	𐤎	
10000	萬	万	丨○○○○				

нумерация имеет очень древнее происхождение, причём известно, что раньше принцип вычитания применялся ещё шире. Так, 8 обозначалось IIX. Само начертание «цифр» было заимствовано римлянами у более ранних обитателей Италии — этрусков. Знак для числа десять у этрусков был ⊣ или ⨯, причём римляне переняли эту последнюю форму. Пять этруски писали ⋁ или ⋀ — это была половина знака для десяти. Этрусское 50, писавшееся, как ↓, обратилось сначала в ⊥, затем в ⊥ и, наконец, в ⌊. Римский знак для ста C произошёл от этрусского знака ⊕, который обратился в Ⓘ, а затем и в C, и т. д.

Интересно отметить, что наряду с принципом сложения и вычитания римлянами употреблялся своеобразный принцип «деления». Так, знак для пяти есть половина знака для X. Более отчётливо этот принцип выступает в двадцатиричной непозиционной системе ацтеков. Число 400 там обозначается так: , 300 = , 200 = и 100 = .

Ближе к позиционной системе стоят системы счисления с мультипликативной формой записи. Таковы старая китайская система, в которой мультипликативный принцип применялся, уже начиная с десятков (табл. 2), индусская система чисел карошти (см. табл. 2), где принцип этот применялся, начиная с сотен, и др. В старокитайской системе 20 или 30 изображались схематически, как 2, 10; 3, 10 и т. п. Сто, тысяча и десять тысяч имели индивидуальные обозначения. Сложные числа обозначались по аналогичной схеме, что и числа, кратные десяти. Число 333 записывалось схематически так: 3, 100, 3, 10, 3. В единообразном обозначении единиц высших и низших разрядов уже можно усмотреть первое приближение к позиционности. Подробнее об этом будет сказано в главе о происхождении позиционной системы. Здесь отметим только, что и в нашей устной нумерации играет большую роль мультипликативный принцип (двадцать = два, десять, триста = три, сто и т. д.).

§ 3. Алфавитные системы нумерации

Наиболее совершенной разновидностью непозиционных систем, не считая систем, основанных на мультипликативном принципе, являются алфавитные системы обозначения чисел. Примерами алфавитных систем могут служить ионийская система нумерации (Древняя Греция), славянская система (кириллица и глаголица), еврейская, арабская, а также грузинская и армянская системы нумерации.

Системой счисления, приближающейся по типу к алфавитной, является египетская иератическая система (см. табл. 1), существовавшая наряду с иероглифической уже в Древнем Египте за 2000 лет

до н. э. Она употреблялась в хозяйственных отчётах и других официальных документах, а также в математических папирусах (записи в обоих древнейших математических папирусах: Московском и Райнда сделаны по иератической системе), тогда как иероглифическое письмо применялось, если можно так выразиться, в «парадных случаях» — для надписей на памятниках и обелисках. Иератическое письмо первоначально возникло из иероглифического в результате сокращений и слияний отдельных символов, естественных при всякой скорописи. Однако при этом числа от 1 до 9, которые обозначались при иероглифическом письме простым повторением символа единицы, получили особые индивидуальные обозначения, т. е. впервые появились особые цифры для чисел первого десятка. Такие же индивидуальные символы образовались для обозначения десятков 10—90, сотен 100—900, тысячи, десяти тысяч и 10^5.

Таким образом, иератическая система счисления принципиально отличалась от иероглифической. На важность этого нового принципа, который можно назвать цифровым, указал ещё в 1911 г. выдающийся русский историк науки В. В. Бобынин [1]). Ч. Бойер недавно поставил цифровой принцип (по его терминологии — ciphirisation) на одну доску с принципом позиционности. «Введение египтянами идеи цифирного обозначения. — пишет Бойер, — представляет собой решающий шаг в развитии нумерации, и в этом отношении их вклад вполне сравним по значительности со вкладом вавилонян, введших позиционный принцип» [2]). Однако, как ни велика роль цифрового принципа, справедливо указанная В. В. Бобыниным, утверждение Бойера является сильным преувеличением. Позиционная система, как мы увидим, имеет неоспоримые преимущества перед системами типа иератической, даже если число применяемых цифр невелико, как это имело место в Вавилоне. Однако цифровой принцип был значительным шагом вперёд по сравнению с иероглифическими нумерациями. Мы будем подробнее говорить о его преимуществах в связи с алфавитной системой обозначения чисел. К тому же типу, что и египетская иератическая, относится и сингалезская нумерация. В самом Египте примерно в VI в. до н. э. получило распространение демотическое письмо, являющееся дальнейшим видоизменением иератического; в Греко-римскую эпоху оно стало в Египте общепринятым.

Алфавитная система нумерации впервые, повидимому, была применена в Греции. Древнейшая надпись, сделанная по этой системе, относится к середине V в. до н. э. (Галикарнасс в Малой Азии). Во всех алфавитных системах числа от 1 до 9, все десятки и сотни обозначаются индивидуальными символами при помощи последова-

---

[1]) См. В. В. Бобынин, Отзыв о сочинениях Н. М. Бубнова, СПБ, 1911.
[2]) Ch. Boyer, Fundamental Steps in the Development of Numeration, Isis, 1944, № 100, т. 35, стр. 158.

тельных букв алфавита (табл. 3). В греческой и славянской нумерации над буквами, означающими цифры, чтобы отличать числа от обычных слов, ставилась черта. Все числа до 999 записывались на основе принципа сложения из 27 индивидуальных знаков для цифр. Так как в обычном греческом алфавите только 24 буквы, то для числовых обозначений были использованы ещё три старые буквы: ϛ (дигамма) для числа 6, ϙ (коппа) для 90 и ϡ (сампи) для 900 (см. первый столбец табл. 3).

Число 444 по этой системе записывалось так: $\overline{\upsilon\mu\delta}$. В римской системе нумерации это число имело бы вид: CDXLIV, а в аттической системе ΗΗΗΗΔΔΔΔΙΙΙΙ.

Уже этот пример показывает неоспоримые преимущества алфавитных систем. То, что алфавитные системы явились нумерацией нового, более высокого типа, доказывается и всем ходом исторического развития. Возникнув в торговых греческих колониях, ионийская нумерация быстро стала распространяться в Аттике, вытесняя освящённую традицией геродианову систему, которую поддерживали и власти, долгое время разрешавшие применять в официальных документах только геродианову нумерацию.

Здесь мы видим ещё одно подтверждение сталинского положения о развитии через борьбу противоположностей, о неодолимости нового. Несмотря на все рогатки и преграды, несмотря на силу традиции, алфавитная система всё шире распространялась по Аттике. Она окончательно вытеснила геродианову после того, как при Птолемее Филадельфе была принята в Александрии.

Однако ряд историков математики, в том числе М. Кантор и Г. Ганкель, считали, что алфавитная система нумерации является шагом назад даже по сравнению с аттической. Отсюда они делали вывод, что греки, которым вообще принадлежит столь значительное место в развитии европейской культуры, для усовершенствования систем счисления решительно ничего не сделали. Такое мнение является совершенно неосновательным. Действительно, требования, которым должна удовлетворять удобная система счисления, таковы: 1) краткость и лёгкость записи, 2) удобство вычислений над числами, записанными в этой системе, 3) лёгкость овладения системой, 4) принципиальная возможность записи в этой системе любого сколь угодно большого числа. Мы видели, что первому требованию ионийская система удовлетворяет, причём запись чисел в этой системе гораздо короче, чем в аттической. Чтобы проверить, насколько трудно производить вычисления в этой системе, французский историк математики П. Таннери в 1882 г. овладел ионийской нумерацией и применил её к выкладкам, необходимым для вычислений в «Измерении круга» Архимеда. Он убедился при этом, что ионийская система имеет практические преимущества, о которых он едва мог подозревать ранее, и что операции в этой системе получаются не намного длиннее наших, если их проводить по современной

Таблица 3

Алфавитное обозначение чисел

	Греческое 1	Славянское: Кириллицей 2	Славянское: Глаголицей 3	Еврейское 4	Сирийское 5	Арабское 6	Грузинское 7	Армянское 8
1	$\bar{\alpha}$	а҃	ⰰ	א	ܐ	ا	ა	Ա
2	$\bar{\beta}$	в҃	ⰱ	ב	ܒ	ب	ბ	Բ
3	$\bar{\gamma}$	г҃	ⰲ	ג	ܓ	ج	გ	Գ
4	$\bar{\delta}$	д҃	ⰳ	ד	ܕ	د	დ	Դ
5	$\bar{\epsilon}$	є҃	ⰴ	ה	ܗ	ه	ე	Ե
6	$\bar{\varsigma}$	ѕ҃	ⰵ	ו	ܘ	و	ვ	Զ
7	$\bar{\zeta}$	з҃	ⰶ	ז	ܙ	ز	ზ	Է
8	$\bar{\eta}$	и҃	ⰷ	ח	ܚ	ح	ჩ	Ը
9	$\bar{\theta}$	ѳ҃	ⰸ	ט	ܛ	ط	თ	Թ
10	$\bar{\iota}$	і҃	ⰹ	י	ܝ	ى	ი	Ժ
20	$\bar{\kappa}$	к҃	ⰺ	כ	ܟ	ك	კ	Ի
30	$\bar{\lambda}$	л҃	ⰻ	ל	ܠ	ل	ლ	Լ
40	$\bar{\mu}$	м҃	ⰼ	מ	ܡ	م	მ	Խ
50	$\bar{\nu}$	н҃	ⰽ	נ	ܢ	ن	ნ	Ծ
60	$\bar{\xi}$	ѯ҃	ⰾ, ⰿ	ס	ܣ	س	ჯ	Կ
70	$\bar{o}$	о҃	ⰿ	ע	ܥ	ع	ო	Հ
80	$\bar{\pi}$	п҃	ⱀ	פ	ܦ	ف	პ	Ձ
90	$\bar{q}$	ч҃, ч҃	ⱁ	צ	ܨ	ص	ჟ	Ղ
100	$\bar{\rho}$	р҃	ⱂ	ק	ܩ	ق	რ	Ճ
200	$\bar{\sigma}$	с҃	ⱃ	ר	ܪ	ر	ს	Մ
300	$\bar{\tau}$	т҃	ⱄ	ש	ܫ	ش	ტ	Յ
400	$\bar{\upsilon}$	у҃	ⱅ	ת	ܬ	ت	უ	Ն
500	$\bar{\phi}$	ф҃	ⱆ, ⱇ	תק		ث	ჭ	Շ
600	$\bar{\chi}$	х҃	ⱈ	תר		خ	ფ	Ո
700	$\bar{\psi}$	ѱ҃	ⱉ	תש		ذ	ქ	Չ
800	$\bar{\omega}$	ѡ҃	ⱊ	תת		ض	ღ	Պ
900	$\bar{ϡ}$	ц҃	ⱋ	ץ		ظ	ყ	Ջ
1000	͵$\bar{\alpha}$	͵а҃	ⱌ	א̈		غ	შ	Ռ
2000	͵$\bar{\beta}$	͵в҃				بغ	ჩ	Ս
3000	͵$\bar{\gamma}$	͵г҃				جغ	ც	Վ
4000	͵$\bar{\delta}$	͵д҃				دغ	ძ	Տ
5000	͵$\bar{\epsilon}$	͵є҃				هغ	წ	Ր
6000	͵$\bar{\varsigma}$	͵ѕ҃				وغ	ჭ	Ց
7000	͵$\bar{\zeta}$	͵з҃				زغ	ჯ	Ւ
8000	͵$\bar{\eta}$	͵и҃				حغ	ჰ	Փ
9000	͵$\bar{\theta}$	͵ѳ҃				طغ	ჱ	Ք
10000	$\overset{\alpha}{M}$	Ⓐ				يغ	ჲ	Օ
20000	$\overset{\beta}{M}$	Ⓑ				كغ		Ֆ

схеме. К мнению П. Таннери присоединился и Т. Хисс. В упомянутой выше статье Бойер развивает дальше мысль о том, что лёгкость вычислений является не столько следствием позиционного принципа записи, сколько следствием схемы вычисления. Это близко к истине по отношению к не слишком большим числам. Нужно, однако, отметить, что современная схема умножения и деления чисел сама основана на позиционности расположения чисел, т. е. в ней используется в другом виде тот же позиционный принцип, что и в нашей нумерации.

То, что грекам приходилось запоминать 27 знаков для цифр вместо наших 10, также не может считаться существенным недостатком системы, так как, во-первых, запоминание это производилось раз и навсегда, а, во-вторых, для чисел не вводилось новых знаков; их обозначения запоминались вместе с алфавитом.

Против алфавитной системы М. Кантор сделал ещё следующее возражение: при нашей системе записи из того, что $2+3=5$, сразу следует, что $20+30=50$, тогда как при алфавитном способе из того, что $\overline{\beta}+\overline{\gamma}=\overline{\varepsilon}$, не видно, что $\overline{\varkappa}+\overline{\lambda}=\overline{\nu}$. Отсюда, по его мнению, следовало, что грекам нужно было запоминать гораздо больше основных частных случаев умножения и сложения, чем нам. Однако процесс счёта имеет дело не только со знаками, но и со словами [1]). Заучивая, например, таблицу умножения, мы запоминаем не то, что символ 2, соединённый знаком умножения с символом 3, даёт символ 6, а заучиваем её в словах «дважды три шесть», которые в случае надобности переводим на знаки. Но словесные обозначения чисел были у греков аналогичны нашим, поэтому грекам было не труднее, чем нам, из того, что дважды три равно шести, заключить, что двадцать на тридцать равно шестистам.

Итак, для записи сравнительно небольших чисел и для оперирования с ними при позиционной схеме вычислений алфавитная система была почти так же удобна, как и позиционная. Но в алфавитной системе непосредственно нельзя было записывать достаточно большие числа. Для этого пришлось к алфавитной системе прибавить новые принципы.

Попытки записать в этой системе числа больше тысячи привели к обозначениям, которые можно рассматривать как зачатки позиционной системы. Так, для обозначения тысячи применялась та же буква, что и для обозначения единицы, но снабжённая чёрточкой слева внизу (см. табл. 3):

$$\overline{\alpha}=1,\quad {}_{,}\overline{\alpha}=1000,\ \ldots,\quad \overline{\theta}=9,\quad {}_{,}\overline{\theta}=9000.$$

При помощи букв со штрихами слева, таким образом, греки могли выразить все числа вплоть до 9999. Число 10 000 обознача-

[1]) Ср. М. Я. Выгодский, Арифметика и алгебра в древнем мире, М.—Л., 1941, стр. 184.

лось знаком $\overset{\alpha}{\text{M}}$; знак $\overset{\beta}{\text{M}}$ означал 20 000 и т. д. Здесь уже применяется мультипликативный принцип. При этом $\overset{\beta}{\text{M}}$ можно было записать ещё как β^{M} или $\text{M}\beta$. Если коэффициент M записывали позади соответственной буквы, то часто он заменялся просто точкой. Например, 43 458 записывалось так: $\overline{\delta.,\gamma\upsilon\nu\eta}$. Этот последний способ записи, применявшийся Диофантом, ближе всего к позиционному.

Наибольшее число, которое можно было записать при помощи ионийской системы счисления, было $10^8 - 1$. Хотя, казалось бы, алфавитная нумерация наталкивала на мысль давать значение цифре не только по её написанию, но и по месту, которое она занимает, однако ни одна алфавитная нумерация не дала начала позиционной системе. Лишь два крупнейших математика древности, Архимед (287—212) и Аполлоний (265?—170), довольно близко подошли к мысли о позиционном принципе обозначения. Архимед в «Исчислении песка» предложил счёт «октадами». Все числа от 1 до 10^8—1 объединяются в первую октаду. Затем 10^8 принимается за новую единицу счёта, и все числа от 10^8 до 10^{16}—1 относятся ко второй октаде и т. д. При этом все числа второй, третьей и последующих октад обозначались так же, как и числа первой октады. Аналогичную группировку дал в своём «Быстросчётчике», до нас, к сожалению, не дошедшем, Аполлоний, только вместо октад он пользовался тетрадами (10^4). Все числа от 1 до 10^4—1 он объединял в первую тетраду, от 10^4 до 10^8—1 — во вторую и т. д. [1]).

И всё же ни Архимеду, ни Аполлонию не пришла мысль о единообразном обозначении всех чисел с помощью 10 знаков (например, 10 первых букв алфавита) по позиционному принципу, ни тем более мысль о введении нуля.

Это обстоятельство, как отмечает и М. Я. Выгодский, объясняется тем, что «ионийская система нумерации в пределах чисел, с которыми греческим математикам приходилось оперировать, вполне удовлетворяла требованиям практики» [2]). Поэтому даже тогда, когда греки уже применяли для дробей шестидесятиричную систему, заимствованную ими у вавилонян, причём пользовались и символом для нуля, они не изменили нумерации целых чисел. Этим же можно объяснить и то, что позиционная система, ставшая известной в Византии уже задолго до Максима Плануда (XIII в. н. э), не получила там всё же распространения, и общеупотребительной продолжала оставаться алфавитная нумерация.

---

[1]) Тот же принцип применяется в приводимом Аполлонием способе умножения, совершенно аналогичном нашему. Умножение двух чисел, кратных десяти или ста, по этому способу сводилось к умножению их «коренных» чисел, т. е. к умножению чисел, выражающих число десятков или сотен в этих числах.

[2]) М. Выгодский, Арифметика и алгебра в древнем мире, стр. 192.

Следы алфавитной нумерации сохранились вплоть до настоящего времени. Так, мы часто нумеруем буквами «пункты» докладов, резолюций и т. д., подобно тому как некогда были занумерованы буквами двадцать четыре песни «Илиады». Однако алфавитный способ у нас сохранился только для обозначения порядковых чисел. Количественные или кардинальные числа мы никогда не обозначаем буквами, тем более никогда мы не оперируем с числами, записанными по алфавитной системе.

Старинная русская нумерация также была алфавитной. Славянское алфавитное обозначение чисел возникло в X в. Введение такого обозначения приписывается составителю славянского алфавита Кириллу (ум. 869). Система обозначения чисел была построена по образцу ионийской, бывшей в ходу у византийцев, причём числовые значения получили лишь те буквы, которые соответствовали буквам греческого алфавита. Так, например (см. табл. 3), буква «буки» (Б) не имела числового значения, значение 2 имела буква «веди»(В), так как она соответствовала букве β греческого алфавита, а «буки» не имела своего прообраза среди греческих букв. Буква «фита» (Ѳ) имела числовое значение 9, хотя она стояла в славянском алфавите на предпоследнем месте, ибо соответствующая ей в греческом алфавите буква θ отвечала числу 9. Этих особенностей совершенно не было во втором славянском способе обозначения чисел — глаголице [1]). Там числовые значения букв идут в строго алфавитном порядке. В обеих системах для выделения в тексте чисел над каждой буквой или над всем числом ставился знак ҃ (титло).

В западноевропейских странах в это время и позже применялась исключительно римская нумерация, принадлежащая к более низкому типу систем счисления.

Для обозначения тысяч в кириллице употреблялись те же буквы, только слева и внизу от них ставился знак ⁘.

В славянском языке сложились две системы наименования высших десятичных разрядов: малое число, в котором названия не шли далее 10^6, и великое число или великое славянское число, куда входили числа до 10^{48}, или 10^{49}, или даже 10^{50} («боле сего несть человеческому уму разумевати»). При этом одни и те же названия обозначали в обеих системах различные числа. Так «тьма» обозначала 10 000 в первой системе и миллион (т. е. тысячу тысяч) во второй; легион в первой системе обозначал 10 тем или 100 000, а во второй — тьму тем, т. е. миллион миллионов (10^{12}), леодр в первой — 10 легионов, т. е. миллион, а во второй — легион легионов (10^{24}). Далее счёт шел на десятки, сотни и т. д. до ста

[1]) Глаголица — одна из славянских азбук, происхождение которой не выяснено точно до сих пор. Возможно, что глаголица предшествовала кириллице. О более ранних обозначениях чисел славянами ничего достоверного не известно.

тысяч тем легионов (10^{47}), а следующей единицей служил леодр леодров (10^{48}), называвшийся вороном. Иногда 10^{50} именовали колодой.

Из одной рукописной грамматики XVII в. известны старинные обозначения высших разрядов в «великом числе словенском». Буквы алфавита, соответствующие числам 1—9, обведённые кружком ○, обозначали тьмы, обведённые кружком из точек — легионы, а кружком из лучей — леодры. Символ служил для обозначения ворона; колода обозначалась [1]).

Несомненно, что обе эти системы нумерации, известные нам из рукописей XVII в., возникли значительно ранее. В русских математических рукописях XVII в. применялась уже современная система нумерации, вытеснявшая алфавитную. Вместе с алфавитной системой из обихода исчезли и описанные устные наименования высших десятичных разрядов.

Подобные двоякие значения названий в зависимости от того, к какой системе принадлежит данное число, существовали долгое время и в Западной Европе. Слово миллион, например, было впервые введено в XIV в. в Италии для обозначения «большой тысячи», т. е. $(1000)^2$. Первоначально оно, повидимому, явилось названием конкретной меры — 10 бочонков с золотом. В XV—XVI вв. это слово распространилось и в других европейских странах. Французский учёный конца XV в. Николай Шюке ввёл слова биллион (byllion), триллион (tryllion), квадриллион (quadrillion), ... , нониллион (nonyllion) для обозначения степеней миллиона: $(1\,000\,000)^2$, $(1\,000\,000)^3$, ... , $(1\,000\,000)^9$. Примерно с середины XVII в. во Франции числа стали разделять на периоды по три цифры в каждом. При этом биллион вместо старого значения $(1\,000\,000)^2 = 10^{12}$ получил значение 10^9. Слова триллион, квадриллион и т. д. стали обозначать соответственно 10^{12}, 10^{15}, ... Однако в Англии, Германии и других североевропейских странах слова эти до сих пор означают 10^{12}, 10^{18}, 10^{24}, ...

§ 4. Поместные или позиционные системы счисления

Первой известной нам системой счисления, основанной на поместном или позиционном принципе, является шестидесятиричная система древних вавилонян, возникшая примерно за 2000 лет до н. э. Вавилоняне записывали все числа при помощи двух знаков: простого «клина» , означающего единицу, и лежачего «клина» , означающего 10. Числа до 60 записывались при помощи повторения этих двух знаков по тому же аддитивному принципу, по

---

[1]) См. В. В. Бобынин, Очерки истории развития физико-математических знаний в России, вып. I, М., 1886, стр. 45—47.

которому строилась, например, египетская система нумерации. Число 32 в этой системе выглядело так: .

Направление письма шло слева направо, причём вначале всегда ставились десятки, а затем единицы. Отдельные клинья при написании чисел, содержащих более четырёх десятков или более четырёх единиц, соединялись в слитные группы (рис. 2).

Число шестьдесят снова изображалось символом , являясь единицей высшего разряда. Далее, для чисел от 60 до 3600—1 повторялись те же обозначения, что и для чисел от 1 до 59, только каждый символ имел в шестьдесят раз большее значение. Например, число 82 записывалось так: .

Однако эта же самая запись могла означать и $1\frac{22}{60}$, или $82 \cdot 60$ и вообще $82 \cdot 60^{\pm k}$. Более того, эта же запись могла соответствовать и числу $60^2 + 22$ и всякому числу вида $60^{\pm k} + 22 \cdot 60^{\pm n}$ и т. п. Таким образом, позиционная запись по шестидесятиричной системе не имела абсолютного характера. Каково действительное значение записанного числа, приходилось всякий раз определять по смыслу задачи. Такой неабсолютный характер записи обусловливался отсутствием в вавилонской системе цифр знака для нуля.

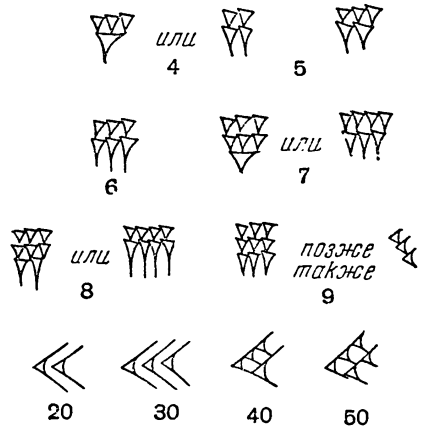


Рис. 2.

Отсутствие нуля на первых порах развития шестидесятиричной системы, когда приходилось оперировать со сравнительно небольшими числами, не было столь ощутительным, как это может показаться. Так, легко подсчитать, что для записи по вавилонской системе чисел от 1 до 3600 нуль нужен только 59 раз (а для записи чисел от 1 до 59 он вообще не нужен), тогда как при записи этих же чисел в нашей десятичной позиционной системе он встречается 917 раз. При оперировании с числами, бóльшими 3600, потребность в нуле возрастает. Поэтому не удивительно, что в более поздних текстах, в которых вавилоняне в связи с потребностями практики, в первую очередь астрономии, оперировали уже с гораздо бóльшими числами, появился междуразрядовый знак , означающий пропуск шестидесятиричного разряда [1]). В конце числа, однако, этот знак никогда не ставился, и абсолютное значение написанного числа определялось только из контекста.

[1]) Первое появление междуразрядового знака относится к персидской эпохе (VI—V вв. до н. э.).

Итак, система счисления вавилонян отличалась от современной десятичной позиционной системы (если отвлечься от различия в основаниях 60 и 10) следующими двумя чертами:

1. Позиционный принцип в ней не был проведён вполне последовательно.

2. Благодаря отсутствию символа для нуля позиционная запись у вавилонян не имела абсолютного характера.

Шестидесятиричная система вавилонян сыграла большую роль в математике и в астрономии. Следы этой системы сохранились до наших дней. Так, мы до сих пор делим час на 60 минут, минуту — на 60 секунд и т. д. Точно так же окружность мы, следуя вавилонянам, делим на 360 частей-градусов.

Вопрос о происхождении этой первой позиционной системы много лет занимает внимание учёных. Существует несколько конкурирующих гипотез, претендующих на объяснение появления этой системы.

М. Кантор первоначально предположил, что сумерийцы (первичное население долины Ефрата) считали год равным 360 суткам и что шестидесятиричная система имеет астрономическое происхождение. Однако в дошедших до нас сочинениях древнего Вавилона встречается лишь солнечный год в 365 дней и лунный год в 354 или 355 дней. Это обстоятельство, а также другие замечания критиков заставили Кантора отказаться от его гипотезы.

По гипотезе Г. Кевича в долине Ефрата встретились два народа, из которых у одного была десятичная система счисления, а у другого основанием системы было число 6 (возникновение такого основания Кевич объясняет особым счётом на пальцах, в котором сжатая в кулак рука означала 6). Благодаря слиянию обеих систем возникло «компромиссное» основание, равное 60. Согласно Леффлеру «благодаря наклонностям сумерийских жрецов к умозрению, их очень рано стали занимать игры с числами; они заметили, что из всех чисел ниже 100 число 60 обладает наибольшим числом малых множителей, как 2, 3, 4, 5, 6. Это открытие побудило их создать для *научных целей систему с основным числом* 60» [1]).

Гипотезы эти совершенно неисторичны; число их можно произвольно увеличить [2]). Последняя же гипотеза является даже антиисторичной, так как системы счисления никогда и нигде не создавались ни учёными, ни тем более жрецами «для научных целей», ни даже отдельными классами, а всегда были результатом длительного исторического развития, результатом творчества всего народа или нескольких народов.

---

[1]) Е. Леффлер, Цифры и цифровые системы культурных народов в древности и в новое время, Одесса, 1913, стр. 33.

[2]) См. об этом примечания И. Ю. Тимченко в книге Ф. Кэджори, История элементарной математики, Одесса, 1918, стр. 313—317.

Более правдоподобна гипотеза о возникновении как основания 60, так и позиционной системы, предложенная в 1927 г. О. Нейгебауером[1]). В основу её положены следующие факты:

1) В эпоху, относящуюся к четвёртому тысячелетию до н. э., система чисел у сумеров была десятичной непозиционной. Имелись индивидуальные обозначения для единицы, 10 и 100, причём знак для 100 («meu») означал на сумерийском языке также неопределённое множество. Таким образом, в это время система счисления у сумеров была примерно такой же, как у египтян, только ещё крайне неразвитой. Кроме того, существовала небольшая группа индивидуальных знаков для дробей $\frac{1}{2}$, $\frac{1}{3}$ и $\frac{2}{3}$.

2) В эпоху расцвета сумерийской культуры, предшествовавшую появлению собственно математических текстов, появляется новый разряд: 60. Он обозначается тем же знаком, что и единица, но только большего размера. В этот период система счисления является шестидесятиричной непозиционной, хотя в ней сохраняется и самостоятельный знак для 100. Система эта сходна по типу с египетской, только в Египте разрядами, имеющими индивидуальные знаки, были 1, 10 и 100, а в Вавилонии — 1, 10 и 60. Разумеется, никакого междуразрядного знака здесь ещё нет, да он и не нужен, так как разряды имеют абсолютные обозначения.

3) В дальнейшем 60 обозначается тем же знаком, что и единица. Единообразный принцип обозначения распространяется и на дроби, однако ещё долгое время сохраняются индивидуальные обозначения для дробей $\frac{1}{2}$, $\frac{1}{3}$ и $\frac{2}{3}$.

Для объяснения этих фактов Нейгебауер рассматривает систему вавилонских мер. Особенно его внимание привлекают меры веса, так как эта система являлась здесь, как и почти всюду, основой денежной системы.

Нейгебауер приходит к заключению, что первоначально существовали две денежные системы у двух народов: сумеров и аккадян, семитского племени, покорившего сумеров. Основной единицей одной из систем был шекель, другой — мина. Каждая из этих денежных единиц давала начало рядам $\frac{1}{3}$, $\frac{1}{2}$, $\frac{2}{3}$, 1, ..., 10.

Обе системы были десятичными. При этом первоначально соотношение между шекелем и миной не было установлено. Оба ряда сосуществовали, служа один для мелких, другой для крупных расчётов. Развитие централизованного Вавилонского государства с единой системой хозяйства привело к сравнительно ранней нормировке денежно-весовой системы. Естественно было установить соответствие так, чтобы дробные части большей единицы, мины

[1]) Ср. О. Нейгебауер, Лекции по истории античных математических наук, т. 1, перев. С. Я. Лурье, М.—Л., 1937, стр. 120—125.

(т. е. $\frac{1}{2}$, $\frac{1}{3}$ и $\frac{2}{3}$ её части), выражались в меньшей единице (в шекелях) в целых числах. По Нейгебауеру, это было осуществлено путём приравнивания дробных частей мины десятикратным шекеля. Таким образом, соотношение между шекелем и миной было установлено 1 : 60 (это соотношение примерно соответствовало соотношению их первоначальных весов).

Сначала соотношение это было абсолютным. Малые и большие единицы отличались друг от друга в написании либо размерами выражавших их знаков, либо сокращёнными названиями, ставившимися после соответствующих единиц.

Со временем система мер веса распространяется на другие области величин. При этом уже не имеет смысла ставить после единиц название той или иной меры веса. Первоначально позиционное обозначение «есть не что иное, как систематический отказ от обозначения единиц меры при письме». Процесс этот происходил бессознательно, иначе нельзя объяснить, почему не был введён знак обозначения недостающего разряда. Самый факт отсутствия в древних текстах такого знака показывает, что «несмотря на то, что числовые знаки были формально одни и те же, при каждом отдельном разряде подразумевалось конкретное обозначение соответствующей меры» [1]).

Описанный процесс можно сравнить с тем, который наблюдается и в нашем языке при именовании денег. Так, вместо того, чтобы сказать: 2 рубля 20 копеек, мы говорим: «два, двадцать». Название соответствующих разрядов здесь подразумевается [2]). Знак отделения на местах пропущенных разрядов появился позже, когда эта система была уже сознательно переработана для нужд математики. Эта последняя стадия, нашедшая своё выражение только в математических текстах, и является завершением создания неабсолютной позиционной шестидесятиричной системы вавилонян.

Таким образом, согласно этой гипотезе основные этапы процесса образования позиционной системы в Вавилоне были таковы:

1) установление количественного соотношения между двумя самостоятельно существовавшими системами мер [3]) и

2) опускание названий разрядовых единиц при письме.

Эти этапы возникновения позиционных систем автор излагаемой гипотезы считает совершенно общими. «Позиционная шестидесятиричная система ... оказалась вполне естественным конечным результатом долгого развития, ничем принципиально не отличающегося от аналогичных процессов в других культурах». Благоприятным обстоятельством, приведшим к тому, что такая система была впервые

---

[1]) О. Нейгебауер, Лекции, стр. 124.

[2]) М. Я. Выгодский, Арифметика и алгебра в древнем мире, стр. 69.

[3]) То, что эти системы мер были первоначально в ходу у двух разных народов (сумеров и аккадян), не существенно.

создана именно в Вавилоне, было то, что «нормировка денежно-весовой системы здесь падает на столь раннюю стадию развития, когда, с одной стороны, существовавшая и в Вавилоне первобытно-десятичная структура ещё лишь частично перешла за сто, а с другой, — натуральные дроби ещё ограничивались маленькой группой $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$»[1]), причём ещё не было выработано регулярных процедур счёта.

В изложенной гипотезе интересно стремление её автора связать процесс возникновения шестидесятиричной позиционной системы с развитием общественной экономики — систем мер, денежного хозяйства и т. п. Однако считать эту гипотезу твёрдо установленной теорией нельзя. Так, поддерживающий её в целом М. Я. Выгодский указывает, что в ней «есть гипотетические элементы: обстоятельства установления денежно-весовых эквивалентов не засвидетельствованы никакими положительными данными»[2]). Ряд возражений против этой гипотезы выдвинул в устных выступлениях И. Н. Веселовский[3]) (например, наличие в большом числе деловых текстов эпохи после Хаммураби непозиционных записей, плохо согласующееся с идеей о происхождении позиционной системы из денежно-весовой системы мер). Востоковед Ф. Тюро-Данжен также полагает, что, вопреки мнению Нейгебауера, появлению шестидесятиричной системы в метрологии должно было предшествовать её наличие в нумерации. Таким образом, общепринятого объяснения появления вавилонской нумерации мы ещё не имеем.

Появление позиционной системы обозначения чисел было одной из основных вех в истории культуры. Оно не могло быть случайным. Подтверждением этому является разновременное и самостоятельное возникновение позиционной системы по крайней мере у трёх различных народов: 1) более чем за две тысячи лет до н. э. в долине рек Тигр и Ефрат у вавилонян, 2) в начале н. э. у племени майя, бывших обитателей полуострова Юкатан в Центральной Америке, и 3) в VIII—IX вв. н. э. в Индии.

Расцвет культуры индейцев майя относится к VI — XIII вв. н. э. У майя были две системы записи чисел: 1) система, подобная египетской, применявшаяся в повседневной жизни, и 2) позиционная абсолютная система, употреблявшаяся главным образом для кален-

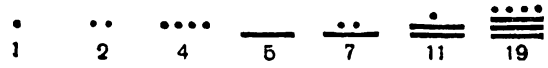
---

[1]) О. Нейгебауер, Лекции, стр. 124.

[2]) М. Выгодский, Арифметика и алгебра в древнем мире, стр. 69—70.

[3]) Основание 60 И. Н. Веселовский связывает со счётом по пальцам и суставам рук, позиционный принцип — с употреблением абака, о чём сказано ниже. И. Тимченко также допускал, что «шестидесятиричное счисление могло произойти от продолжения такого счёта на правой руке, а затем на другой стороне суставов правой и левой руки в обратном порядке», но считал возможным, что оно возникло из смешения 4-ричной и 15-ричной систем (встречающихся, например, в Бенгалии). См. его примечания к книге Ф. Кэджори, История элементарной математики, Одесса, 1917, стр. 316—317.

дарных расчётов, характерной особенностью которой было наличие нуля, символом для которого служило изображение полузакрытого глаза. Основанием системы служило число 20, хотя имелись и сильные следы пятиричной системы. Первые 19 чисел получались путём комбинации знаков точки (·) для единицы и черты (—) для пяти и записывались, например, так:



20 является единицей нового разряда, которая называется уинальс, или 20 дней, и обозначается знаком для единицы, надписанным над знаком для нуля. Однако единицу следующего разряда образуют не 20, а 18 уинальсов, называемые туном (360 дней). Это — единственное отступление от двадцатиричного принципа в системе майя. Оно объясняется тем, что год майя делили на 18 месяцев, по 20 дней в каждом, плюс ещё пять дней. 20 тунов образуют катун или 7200 дней, 20 катунов образуют единицу пятого разряда — цикл и, наконец, 20 циклов составляют большой цикл, равный 2 880 000 дням.

Таким образом, единицами различных разрядов в системе майя были: 1, 20, $20 \cdot 18$, $20^2 \cdot 18$, $20^3 \cdot 18$, ...

В своих календарных и хронологических расчётах майя оперировали очень большими числами. Наибольшее число, найденное в их документах, есть 12 489 781. Запись его в системе майя схематически будет выглядеть так:

$$12\,489\,781 = 4(18 \cdot 20^4) + 6(18 \cdot 20^3) + \\ + 14(18 \cdot 20^2) + 13(18 \cdot 20) + 15 \cdot 20 + 1.$$

Родоначальницей нашей современной нумерации была, повидимому, индусская система. К сожалению, нам очень мало известно о том, как и когда в Индии появилось обозначение чисел по позиционной системе. Работа исследователей очень трудна из-за большого количества подложных надписей. Так, из 17 древних цитат, содержащих позиционные записи, только две оказались неподдельными,

До возникновения позиционной системы в некоторых частях Индии пользовались цифрами карошти (kharosthi), наиболее ранние известные образцы которых найдены были в районе восточного Афганистана и Северного Пенджаба и относятся, вероятно, к III — I вв. до н. э. Это была десятичная непозиционная система с индивидуальными символами для 1, 4, 10, 20 и 100 (см. табл. 2). Особая роль чисел 4 и 20 в системе показывает, что они являлись узловыми. Числа 200, 300 и т. д. обозначались при помощи цифры 100 и приписывания справа соответственно значка для двух или трёх. Таким образом, начиная со 100, в системе действовал мультипликативный принцип. Видеть в цифрах карошти прообразы наших цифр не приходится.

Наряду с числами карошти с древнейших времён в Индии существовала другая система обозначения, знаки которой сходны с буквами так называемого алфавита брами (см. цифры из надписи в пещере Назик, табл. 2). В этой системе имелись специальные знаки для 9 первых чисел, для десятков 10—90 и для чисел 100 и 1000 [1]). Для обозначения 200, 300, 2000 или 3000 писались знаки для 100 или 1000 и приписывались к ним две или три чёрточки. Аналогичным образом числа от 400 до 900 и от 4000 до 70 000 (чи́сла больше этого в известных нам записях не встречаются) записывались в виде сочетания знаков для 100 и 1000 со знаками для 4—9. Схематически запись числа 3451 по этой системе можно выразить так: 3 · «1000» 4 · «100» 5 · «10» 1.

Такая система цифр существовала вплоть до конца XIX в. на Цейлоне, куда индусская культура была занесена вместе с буддизмом в III в. н. э. и где она сохранилась почти без изменения.

Происхождение цифр брами в точности не известно, но есть основания думать, что они арамейского происхождения [2]). Быть может, цифры брами явились первичными формами, из которых развились позднее наши цифры.

В Индии существовала и третья система обозначения чисел, словесная, о которой мы скажем далее.

Запись в позиционной десятичной системе с употреблением знака нуля появилась в Индии, вероятно, около 500 г. н. э.; возможно, что знак нуля известен был Ариабхатте (476—550) [3]). Однако первая точно датированная надпись, в которой встречается знак

---

[1]) Предполагают, что сначала эти цифры, называемые сингалезскими, были начальными буквами соответствующих имён числительных.

[2]) Арамеи — аравийская семитическая народность, во второй половине 2-го тысячелетия до н. э. населявшая территории Сирии и части Месопотамии и создавшая там ряд государств.

[3]) Знак нуля в виде точки встречается в так называемой Бахшалийской рукописи, точное время составления которой не известно. Различные исследователи датируют её по-разному — от II в. н. э. до VIII и IX вв.

нуля, относится к 876 г.: в ней число 270 записано было в виде ২৭০[1]). Как же перешли индусы к абсолютной позиционной системе?

Н. М. Бубнов связывал этот переход с употреблением в Индии и других странах Древнего Востока счётной доски, абака. Доска эта имела продольные желобки, каждый из которых соответствовал определённому десятичному разряду. В эти желобки помещались жетоны, которые были первоначально немеченными и указывали, таким образом, число единиц соответствующего разряда.

Согласно Н. Бубнову, наши числительные и цифры в конечном итоге урало-алтайского происхождения. От урало-алтайских народов они распространились далее, в частности в Халдею (юго-восточная часть Месопотамии). Отсюда в III в. до н. э. цифры эти, с одной стороны, перешли в Индию, где и употреблялись без нуля и без поместного значения, а с другой стороны — в Грецию, где попали на ранее немеченные жетоны греческого абака. Таким образом, для счёта на абаке стали употреблять меченные жетоны, жетоны со знаками цифр от 1 до 9. Здесь же к ним был присоединён десятый пустой жетон (сипос), означавший отсутствие единиц определённого разряда. Из Греции абак попадает на Восток и на Запад. В Индии, где числовые знаки греческого абака были уже известны, но без значения по положению, они приобретают таковое, переходя с жетонов на бумагу в том же порядке, в каком они располагались на абаке. Нужно было только уметь обозначать пропуск того или иного десятичного разряда. Для этого и начали изображать немеченный жетон, представляющий собой кружок с дыркой посредине, так сказать, материализованную модель нуля. Его сначала обозначали жирной точкой, а затем стали писать кружок ○.

Гипотеза эта не лишена остроумия, однако она не подтверждается историческими фактами. Наоборот, против неё можно выставить следующие существенные возражения:

1) На всех дошедших до нас античных рисунках греческий абак изображается с немеченными жетонами. Поэтому нет основания полагать, что у древних греков были меченные жетоны. Наоборот, примеры русских счётов, китайского сван-пана, римского абака показывают, что меченные жетоны совершенно не нужны ни для фиксирования числа на такой счётной доске, ни для производства операций. Известно лишь, что абак с меченными жетонами существовал и получил широкое распространение в средние века.

2) Очень мало вероятно, чтобы на протяжении длинного периода странствования по Индии и Греции арамейские цифры сохранились без изменения.

---

[1]) См. D. E. Smith and L. C. Karpinsky, The hindu-arabical numerals, N.-Y., 1911, стр. 43—44, 52.

3) Абак с древнейших времён был в употреблении у египтян, греков, китайцев, римлян, а между тем ни один из этих народов не пришёл к позиционной системе [1]).

Более правдоподобно предположить, что и абак и позиционная система возникли из одного и того же источника — группового счёта и благодаря одним и тем же историческим процессам.

Возникновение позиционной системы можно представить следующим образом. Принцип позиционности является по существу соединением двух принципов: 1) мультипликативности и 2) опускания при письме разрядовых единиц. Завершается позиционная система введением нуля. Для объяснения происхождения позиционного принципа прежде всего следует объяснить появление мультипликативной формы записи, являющейся, кстати, одновременно основой изображения числа на абаке.

Разберём сначала, чем принципиально отличается мультипликативная форма записи от аддитивной. С чисто алгебраической точки зрения запись, например, числа 30 в виде $\mathrm{III_X}$ или $\mathrm{X^{III}}$ является выражением закона дистрибутивности. Действительно:

$$\mathrm{XXX} = \mathrm{X} + \mathrm{X} + \mathrm{X} = (\mathrm{I} + \mathrm{I} + \mathrm{I})\,\mathrm{X} = \mathrm{III_X} \text{ или } \mathrm{X^{III}}.$$

С другой стороны, запись вроде $\mathrm{III_X}$ выражает тот факт, что при счёте десятки принимаются за новые единицы. То же имеет место и при счёте сотен, тысяч и т. д. Итак, мультипликативная форма записи наиболее отчётливо отражает тот факт, что при счёте определённое множество единиц первого разряда принимается за единицу следующего разряда, определённое множество единиц второго разряда принимается в свою очередь за единицу третьего разряда и т. д. Это достигается тем, что для выражения известного количества единиц различных разрядов применяются одни и те же числовые символы, после которых отмечается, к какому разряду принадлежат сосчитанные единицы. Этой же записью подчёркивается, что объектами счёта могут быть элементы любой природы (вещи, определённые множества вещей, десятки их, сотни и т. д.), а это в свою очередь выражает важнейшее свойство отвлечённого числа быть общей формой, свойственной самому различному конкретному бытию.

Но как раз такой способ счёта, как мы отмечали, имеет место при счёте числами-совокупностями. Так, африканские негры, ведущие счёт на камешках или орехах, складывают их в кучки по 5 предметов в каждой. Пять таких кучек они объединяют в новую кучу и т. д. Очевидно, здесь сначала ведётся счёт камешков, затем

---

[1]) Ср. примечания И. Тимченко к цит. книге Кэджори, стр. 318—320. — Следует отметить, впрочем, что И. Ю. Тимченко полагал, что «идея поместного значения знаков, весьма вероятно, родилась при употреблении абака, даже и не снабжённого меченными жетонами» (там же).

кучек, потом куч и т. д. При таком способе счёта подчёркивается то обстоятельство, что с кучами нужно поступать так же, как и с камешками. Точно так же ведёт счёт и племя Центральной Африки — йорубы с тою лишь разницей, что объектами счёта у них являются раковины-каури, которые складываются в кучи по 20 предметов в каждой. Интересно, что само слово считать означает у них буквально «сметать в кучу», «сгребать». Точно так же у древних греков, различавших арифметику как науку о числе от логистики — искусства счёта, слово λογος имело своим корнем слово λεγ, что означает собирать.

Иллюстрацией дальнейшего развития счёта, приводящего к мультипликативной системе, может служить приводимый у Н. Н. Миклухи-Маклая пример счёта у туземцев Новой Гвинеи. Чтобы сосчитать количество бумажек, обозначавших число дней до возвращения корвета «Витязь», папуасы поступали следующим образом: «первый, раскладывая кусочки бумаги на колене, при каждом обрезке повторял „каре, каре“ (один); другой повторял слово „каре“ и загибал при этом палец, прежде на одной, затем на другой руке. Насчитав до десяти и согнув пальцы обеих рук, он опустил оба кулака на колени, проговорив „две руки“ причём третий папуас загнул один палец руки. Со вторым десятком было сделано то же, причём третий папуас загнул второй палец; то же самое было сделано для третьего десятка» [1]).

Подобным же образом происходит счёт стад у южно-африканских племён (пример этот приводится Цейтеном). Для такого счёта нужны три человека: первый поднимает один за другим десять пальцев своих рук при прохождении каждой головы стада и постоянно повторяет тот же счёт до десяти. Второй считает таким же образом получаемые при этом десятки, третий — десятки, полученные вторым, т. е. сотни. Подобный способ счёта имел место и в других странах. Пример этот проливает свет на происхождение и абака и позиционной системы. В самом деле, если заменить пальцы первого, второго и третьего считающих камешками, помещёнными в различные желобки, или бусами, нанизанными на три проволоки, то получится простейший абак, причём как раз в том виде, в каком он возник. С другой стороны, если обозначить пальцы считающих символами I, X, C, то при перенесении некоторого числа с пальцев на бумагу мы получим мультипликативную форму записи. Число 323 запишется при этом по схеме 3C2X3.

Так как стадия счёта числами-совокупностями является совершенно общей, то она, конечно, имела место и в Индии. С древнейших времён, как мы видели, в Индии существовали мультипликативные числовые системы. Действительно, и система карошти и система

---

[1]) Н. Н. Миклухо-Маклай, Путешествия, т. I, стр. 58, Издательство АН СССР, 1940 г.

брами были построены по этому принципу. Таким образом, большие числа записывались в Индии по той же схеме, что и в Вавилонии, до того момента, как там стали опускать названия разрядов.

Следует иметь в виду также высокий интерес (и не только среди учёных) в Индии к проблеме записи любого числа. Так, в Лилаватистара, знаменитом произведении буддийской литературы, описывается состязание между женихами прекрасной Гопы (госпожи земли). Предметом состязания были письменность, арифметика, борьба и искусство метания стрел. Почти половина описания посвящена испытаниям по арифметике. Состязающиеся должны были, например, найти средство для выражения чисел, бóльших ста коти (1 коти $= 10^7$). Победитель, Сарватасидда, придумал шкалу чисел, идущих в геометрической прогрессии со знаменателем 100, последним членом которой было число $10^{7+9\cdot 46}$, содержащее 421 нуль. После этого он вычислил число «первичных атомов», заключённых в единице длины, для чего также составил таблицу обозначений чисел.

В Индии имелось и ещё одно благоприятное обстоятельство для возникновения позиционной системы. Мы упоминали уже о третьей, словесной системе обозначения чисел, находившей применение в трудах по астрономии и математике. Система эта возникла не позднее VI в. н. э. Единица в ней обозначалась каким-либо из слов «луна», «земля», «брама» и т. д., являющихся названиями предметов, встречающихся в единственном числе, два — каким-либо из слов «близнецы», «глаза», «руки», пять — словом «чувства» или «стрелы» (пять стрел Камадевы, бога любви индусской мифологии) и т. п. Обозначение чисел в этой системе строилось по позиционному принципу. Например, число 867 писалось: «giri — raşa — vasu», т. е. горы (7) — запахи (6) — боги (8), при этом запись следовала от единиц низшего разряда к единицам высшего. Кроме того, в санскритском языке (игравшем у индусов роль средневековой латыни) имелись специальные названия всех разрядов вплоть до 10^{16}. Например, число 86 789325 178 читалось по-санскритски так: 8 kharva, 6 padma, 7 vyrbuda, 8 koti, 9 prayuta, 3 laksha, 2 ayuta, 5 sahasta, 1 gata, 7 daçan, 8. Такой способ обозначения подчёркивал равноправность разрядов. Нужно было только выработать систему записи, которая соответствовала бы уже существующему устному наименованию чисел. Такая система явилась дальнейшим развитием способа записи чисел по мультипликативному принципу.

Процесс опускания названий разрядовых единиц при письме мог итти в Индии так же, как и в Вавилоне. Для завершения позиционной системы нехватало последнего шага — введения нуля. Но при небольшом основании, каким являлось число десять, и при оперировании со сравнительно большими числами, особенно после того, как названия разрядовых единиц перестали отмечать, такое введение стало необходимым. При этом совершенно не существенно, был

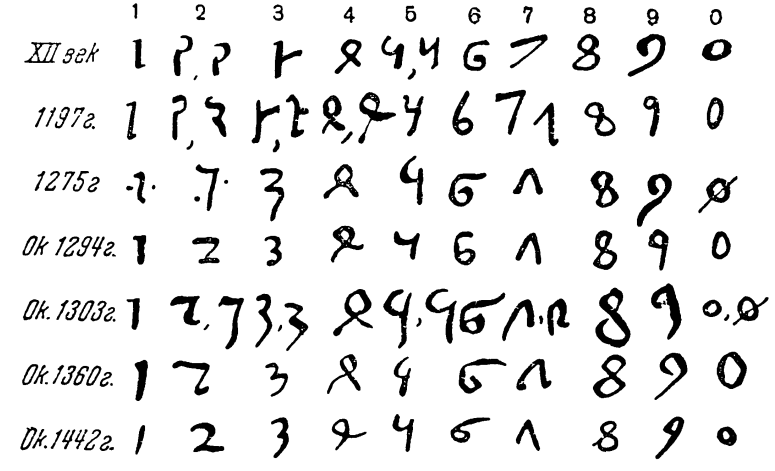
ли первоначально символ нуля изображением пустого жетона абака или видоизменением простой точки, которую могли ставить на место пропущенного разряда. Так или иначе, но введение нуля было совершенно неизбежным этапом закономерного процесса развития, приведшего к созданию современной позиционной системы.

§ 5. Распространение позиционного принципа записи чисел в Западной Европе и в России

Нам остаётся проследить, как индусская позиционная система попала в Европу и как и когда она стала общепринятой у нас в России.

Принцип поместного значения распространился из Индии в другие страны. Некоторые народы переняли у индусов только этот принцип, сохранив своё старое начертание цифр (Китай), другие заимствовали у индусов и их цифры (Тибет, Монголия, народы Ближнего и Среднего Востока). Наиболее ранние рукописи на арабском языке, содержащие позиционную запись чисел, относятся к 874 и 878 гг. В самой Индии, в разных её областях написание цифр было очень различным. Различны были и цифры, распространённые в странах Восточного халифата и в мавританских государствах, расположенных на территории современной Испании. Восточно-арабские цифры впоследствии распространились по всему мусульманскому востоку, где употребляются и до сих пор в несколько видоизменённой форме. А цифры, бывшие в ходу в мавританских государствах, так называемые цифры «губар» (табл. 4, 1-я строка), стали прямыми родоначальниками наших цифр.

Таблица 4



При этом, однако, неясным остаётся вопрос, откуда произошли цифры «губар»? Если они индусского происхождения, то они могли

дойти до Испании только через страны Передней Азии. Как могла некоторая разновидность индусских цифр попасть непосредственно в мавританские государства, «перепрыгнув» страны Передней Азии?

Теория Вёпке, считавшаяся одно время общепринятой, объясняет эти факты следующим образом.

Ещё во II в. до н. э. благодаря установившимся торговым сношениям между Индией и Александрией индусские цифры (без нуля и поместного принципа) проникли в Александрию, а оттуда уже в Рим, в западную часть Африки и в Испанию. Подтверждением этой части своей теории Вёпке считал тот факт, что начертание цифр, сильно напоминающих цифры «губар», имеется в «Геометрии» римского учёного Боэция (480?—524). Боэций в этой книге говорит об абаке, устройство которого он приписывает пифагорейцам. Для счёта на этом абаке употребляются не камешки, а жетоны или апексы с начертанными на них цифрами. Сами эти цифры получили впоследствии название апексов. Они-то и походили по форме на цифры «губар». Позднее в Индии появились принцип поместного значения и знак нуля, которые и были заимствованы народами Среднего и Ближнего Востока вместе с новым начертанием цифр. В мавританских государствах употребляли для записи чисел те цифры, которые уже давно существовали в Испании, а знак нуля и поместный принцип обозначения были заимствованы маврами у своих восточных единоверцев.

К народам Европы начертание цифр и поместный способ обозначения перешли из Испании. Цифры эти назывались по-арабски «губар», т. е. пыль, песок. По мнению автора гипотезы, такое название служило напоминанием об индусском происхождении этих цифр (индусы записывали цифры на пыли или песке). С другой стороны, в самой Индии начертание цифр подверглось дальнейшему изменению, чем и объясняется отличие цифр «губар» от современных индусских цифр «девангари».

Слабыми местами теории Вёпке является то, что 1) наличие индусских цифр в Александрии во II в. до н. э. и даже много позднее не подтверждается никакими историческими фактами и 2) «Геометрия» Боэция, на которую ссылается автор, как теперь установлено, является скорее всего неподлинной и относится примерно к XI в. н. э. Эту гипотезу Вёпке раскритиковал Н. М. Бубнов в своей книге «Арифметическая самостоятельность европейской культуры» (Киев, 1908). Однако собственная гипотеза Бубнова является не лучше обоснованной, чем гипотеза Вёпке. Известный русский историк математики В. В. Бобынин подверг решительной критике гипотезу Н. М. Бубнова в «Отзыве о сочинениях Н. М. Бубнова и т. д.» (С.-Петербург, 1911). В. В. Бобынин писал по поводу теории Бубнова: «История наших цифр представляет не более, как ряд предположений, перемежающихся с произвольными допущениями, произ-

водящими иногда, вследствие предшествующего употребления метода внушения, впечатление как бы чего-то доказанного».

В настоящее время под руководством С. П. Толстова ведутся раскопки древнего Хорезма — крупнейшего культурного государства древности, находившегося на территории нашего Советского Союза. Можно надеяться, что раскопки эти прольют дополнительный свет на происхождение наших цифр.

Таким образом, мы до сих пор не имеем исторически обоснованной гипотезы, которая достаточно удовлетворительно объясняла бы происхождение наших цифр.

Однако бесспорно, что народы Европы заимствовали свою систему счисления у мусульманских государств, находившихся на территории современной Испании. В X в. культура мавританских государств начинает оказывать всё большее влияние на Европу. В частности, в Европу начинают проникать цифры губар, тогда как до того времени употреблялись по преимуществу римские цифры. Искусство письма было очень мало распространено в Европе того времени, кроме того, письменный счёт при помощи римских цифр крайне неудобен (пусть читатель для примера попробует перемножить два четырёхзначных числа, записанных римскими цифрами), поэтому для вычислений пользовались счётной доской — абаком.

Первое введение абака в Европе обычно связывается с именем Герберта (впоследствии папа Сильвестр II), наиболее выдающегося европейского математика X века (ум. 1003). Герберт написал два сочинения: «Правила вычисления с помощью абака» и «Книжка о делении чисел», в которых он излагал современные ему методы вычислений. Сохранились сведения о том, что по его заказу был изготовлен абак в виде кожаной счётной доски, имеющей 27 вертикальных столбцов, и к нему роговые марки с выбитыми на них девятью первыми числовыми знаками (апексами). По другим сведениям столбцов было тридцать, причём из них три предназначались для дробей, а остальные 27 разделялись на группы по три столбца в каждой. Столбцы были помечены буквами: M (monas) или S (singularis), D (decem, 10), C (centum, 100); далее ставились те же буквы, но с чертой наверху, причём каждая имела уже в тысячу раз большее значение. Например, $\overline{C}$ было пометкой столбца для 100 000. Последователи Герберта получили название абацистов. В течение ближайших веков абак значительно видоизменился: нумерованные жетоны были заменены ненумерованными, вертикальные желобки — горизонтальными. Такого рода абак был распространён в Германии, Франции и Англии.

Хотя первая запись арабо-индусскими цифрами, но без употребления нуля встречается в рукописях испанского монастыря Альбельдо ещё в 976 г. (так называемый codex vigilianus), а в рукописи X в. из Сан-Гала (университетская библиотека в Цюрихе) имеется уже знак нуля, однако арифметические приёмы народов Среднего

и Ближнего Востока начинают укрепляться в Европе, только начиная с XII столетия. В этом отношении имел колоссальное значение перевод арифметического труда замечательного хорезмского учёного Магомета сына Мусы-ал-Хваризми (т. е. из Хорезма; ум. около 840), в котором был изложен позиционный способ обозначения чисел [1]). Сам этот способ получил название алгорифма (искажённое прозвище ал-Хваризми). Большую роль сыграли также компилятивная «Книга об алгорифме»(Liber alghoarismi) еврейского учёного XII в. Иоанна Севильского, популярные сочинения по арифметике Александра де Вилла Деи и Джона Галифакса или Сакробоско, живших в середине XIII в. Образовалась целая школа арифметиков, придерживавшихся новых способов обозначения чисел и оперирования ими; она получила название школы алгорифмиков. Алгорифмики не употребляли абака при вычислениях. Они учили наряду с производством первых четырёх действий арифметики ещё и извлечению квадратного корня, а также применяли шестидесятиричные дроби, в то время как абацисты пользовались римскими двенадцатиричными дробями.

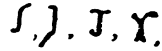
Новая нумерация не была воспринята сразу. Наоборот, она встретила ожесточённое сопротивление и со стороны официальной схоластической науки того времени и со стороны отдельных правительств. Так, в 1299 г. во Флоренции купцам было запрещено пользоваться индусскими цифрами в бухгалтерии и приказано пользоваться либо римскими цифрами, либо писать числа полностью словами. В официальных бумагах вплоть до XVIII в. разрешалось употреблять только римские цифры.

Достоинства позиционной системы, ясные для её пропагандистов, обнаруживались для широких кругов не сразу. Счёт на абаке долгое время сохранял в глазах многих преимущество. Здесь имели значение, кроме приверженности к рутине, дороговизна бумаги, производство которой было введено в Европе лишь в XII в., недостаток письменных принадлежностей (карандаши появились лишь в XVI в.), весьма постепенное совершенствование самих приёмов действия в новой системе счёта, особенно умножения и деления, и, наконец, чрезвычайное отличие в форме записи одних и тех же цифр у различных писателей [2]) вплоть до изобретения в XV в. книгопечатания.

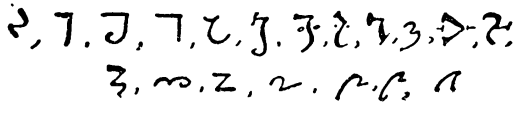
---

[1]) Латинский перевод этого сочинения ал-Хваризми, сделанный в середине XII в., опубликован Бонкомпаньи: Trattati d'Aritmetica, Roma, 1857.

[2]) Вот как, например, варьировали в разных рукописях цифры для единицы:



и для двойки:



Однако ещё в XIII в. новая система начала распространяться среди итальянских купцов. Преимущества её, связанные с последовавшим упрощением арифметических операций, были столь велики, что, несмотря на все препятствия, позиционная система постепенно вытеснила старые способы счёта и старую нумерацию.

Интересным примером торжества новой нумерации явились записи, сделанные с помощью римских цифр, но с употреблением нуля и позиционного принципа. Так, Н. Окреат на рубеже XI—XII вв. писал III III (т. е. 33) или I. 0. VIII. IX (т. е. 1089) и т. д. [1]).

Леонардо Пизанский, или Леонардо Фибоначчи, в своём сочинении «Liber abaci» (1202) [2]) выступил убеждённым сторонником новой нумерации: «Девять индусских знаков, — писал он, — суть следующие: 9, 8, 7, 6, 5, 4, 3, 2, 1. С помощью этих знаков и знака 0, который называется по-арабски zephirum, можно написать какое угодно число». Здесь словом zephirum Леонардо передал арабское слово as-sifr, являющееся дословным переводом индусского слова sunya, т. е. пустое, служившего названием нуля. Слово zephirum дало начало французскому слову zéro (нуль) и итальянскому слову zero. С другой стороны, то же арабское слово as-sifr было передано через ziffer, откуда произошли французское слово chiffre, немецкое ziffer, английское cipher и русское цифра [3]). Вплоть до середины XVII в. это слово употреблялось специально для обозначения нуля. Например, в «Арифметике» Магницкого цифрой называется только нуль. Латинское слово nullus (никакой) вошло в обиход для обозначения нуля в XVI в. [4]).

В Германии, Франции и Англии новые цифры до второй половины и даже до конца XV в. почти не употреблялись. Первые монеты с индусскими цифрами появились в 1424 г. в Швейцарии [5]), в 1484 г. — в Австрии, в 1485 г. — во Франции, в 1489 г. — в Германии и в 1551 г. — в Англии. На могильных плитах эти цифры появились впервые в Бадене (1371) и Ульме (1388). В 1488 г. была напечатана книга «Об искусстве счисления» («De arte numerandi»), известная также под названием «Algorismus», в которой без примеров и доказательств сообщались правила «индусской» арифметики.

---

[1]) D. Smith and L. Karpinsky, The hindu-arabical numerals, стр. 119—120.

[2]) Слово «абак» стало в то время обозначать уже арифметику вообще, и таким образом, сочинение Леонардо — это «Книга по арифметике», а не о счётной доске — абаке.

[3]) Характерно, что в разгар борьбы алгорифмиков и абацистов слова «алгорифм» и «цифра» нередко служили насмешливыми синонимами для какой-либо бесполезной, пустой вещи!

[4]) Термины nulla figura, nullus circulus (никакая фигура, никакой кружок) для обозначения «нуля» появляются в XII в. в латинских переводах и обработках арифметических сочинений на арабском языке.

[5]) В Сицилии, тесней связанной с арабскими государствами, индусские цифры на монетах появляются не позднее 1138 г.

Книгу эту обычно приписывают упоминавшемуся уже раньше Джону Галифаксу, именуемому чаще Сакробоско. Лишь в XVI—XVII вв. новая нумерация почти полностью вытесняет старую. Однако ещё во второй трети XVI в. числа в календарях обычно печатались римскими цифрами.

В России первая дошедшая до нас математическая рукопись восходит к началу XII в. Это — «Кирика Диакона и Доместика Антониева монастыря учение, им-же ведати человеку числа всех лет». Числа в этой рукописи выражались в алфавитной системе нумерации. Это же относится и к спискам знаменитого юридического памятника, «Правды Русской», относящимся к XIV—XV вв. Новая система нумерации получила распространение в России лишь немногим позднее, чем в Западной Европе, где с нею смогли познакомиться ранее. Уже во всех без исключения математических рукописях XVII в. применялась позиционная десятичная нумерация. Как писал В. В. Бобынин, «Следы прежнего употребления древней греко-славянской системы встречаются только в древнейших из них, да и то в таких слабо выраженных формах, как пояснение значения арабских цифр соответствующими славянскими или встречающиеся время от времени обозначения данных чисел славянскими цифрами одними или же вместе с арабскими. Рукописи второй половины XVII столетия не содержат в себе даже и этих незначительных следов» [1]). В широкий обиход новая нумерация вошла, однако, не сразу.

В печатных сочинениях на славяно-русском языке индусские цифры появились впервые при нумерации страниц в двух книгах духовного содержания, изданных в Венеции в 1611 г. В книге, изданной в русской типографии («Псалтырь», напечатанная в местечке Евю), индусская нумерация страниц впервые встречается в 1638 г. В 1647 г. в Москве была издана книга «Учение и хитрость ратного строения пехотных людей», в которой все цифры на чертежах и в ссылках в тексте на чертежи были уже индусскими. Однако ещё долгое время в книгах приводились как «числа русские», так и «цифирные», т. е. индусские. Ещё в 1702 г. «Юрнал» об осаде Нотебурга, выпущенный в 2000 экземплярах, в 1000 экземпляров имел арабо-индусские, а в 1000 экземпляров — славянские цифры.

В знаменитом руководстве «Арифметика, сиречь наука числительная. С разных диалектов на славянский язык переведенная, и во едино собрана и на две книги разделена. В лето от сотворения мира 7211, от рождества Бога Слова 1703. Сочинися сия книга через труды Леонтиа Магницкого», по которому учился великий русский учёный М. В. Ломоносов, обозначения страниц — славянские, но вычисления в тексте производятся исключительно на

---

[1]) В. В. Бобынин, Очерки истории развития физико-математических теорий в России, вып. I, стр. 43.

Арїѳметїка,

сирѣчь наука числительнаѧ.

Съ разныхъ дїалектωвъ на славенскїй языкъ
преведенаѧ, и во едино собрана, и на двѣ
книги раздѣлена

Нынѣ же повелѣнїемъ бл҃гочестивѣйшагω
великагω г҃дрѧ нашегω ц҃рѧ и великагω
кн҃зѧ Петра Алеѯїевича всеѧ великїѧ
и малыѧ и бѣлыѧ рωссїи самодержца:
При бл҃городнѣйшемъ великомъ г҃дрѣ нашемъ
ц҃ревичѣ, и великомъ кн҃зѣ Алеѯїи
Петровичѣ, в бг҃оспасаемомъ ц҃рствующемъ
великомъ градѣ москвѣ тупографскимъ
тисненїемъ ради ωбученїѧ мудролюбивыхъ
рωссїйскихъ отрωкωвъ, и всѧкагω чина
и возраста людей на свѣтъ произведена
первое, въ лѣто ѿ сотворенїѧ мїра
҂зсаі, ѿ рж҃тва же по плоти
бг҃а слова ҂аѱг, індикта аі,
м҃ца іаннуарїа.

Сочинисѧ сїѧ книга чрез труды Леонтїа Магницкагω:

Титульный лист «Арифметики» Магницкого.

индусских числах. Определение нумерации там даётся следующее: «Что есть нумерацио: нумерацио есть счисление еже совершенно вся числа речию именовати, яже в десяти знаменованиях или изображениях содержатся и изображаются: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0». Заметим, между прочим, что нумерация в то время считалась ещё пятым действием арифметики.

Наиболее ранние русские монеты с индусскими цифрами — золотые монеты достоинством в $^1/_4$ червонца с датой 1654 г. Чеканились они в основном не для денежного обращения, а для дарений, наград и т. п. Непосредственно затем на обращавшихся в нашей стране западноевропейских талерах («ефимках») поставлены были клейма с датой 1655 г. При Петре I индусские цифры на монетах полностью вытесняют славянские, в последний раз появившиеся на медных монетах 1718 г. [1]).

В послепетровские времена славянские цифры быстро исчезли из обихода.

§ 6. Дроби

В современной математике дроби вводятся как пары целых чисел (m, n), для которых известным образом определено отношение равенства, подчиняющееся законам рефлексивности, симметричности и транзитивности, а также определены правила действия [2]). При этом целые числа можно рассматривать как частный случай таких дробей, а операции над целыми числами — как частный случай операций над дробями. После такого расширения области целых чисел до области рациональных чисел (или пар целых чисел) становится разрешимым каждое уравнение $ax = b$, где a, b — целые и $a \neq 0$.

Однако в действительности дроби возникали не как результат деления целых чисел; тем более не были они созданы для того, чтобы операция деления, обратная операции умножения, была всегда возможной.

Если бы дроби появились в результате деления целых чисел, то все они были бы с самого начала логически однородны, что отражалось бы в их трактовке и в обозначениях. Исторически же это было не так. Чтобы убедиться в этом, достаточно просмотреть прилагаемую здесь таблицу египетских дробей (рис. 3).

Во-первых, мы видим, что египтяне имели обозначения только для дробей вида $\frac{1}{n}$ и для некоторых дробей вида $\frac{n-1}{n}$. При $n \geqslant 5$ все дроби $\frac{1}{n}$ обозначались вполне единообразно при помощи символа $\backsim$, обозначающего «часть», под которым подписывался

---

[1]) По данным И. Г. Спасского.

[2]) О трактовке дробей с этой точки зрения см. в этой книге статью И. В. Проскурякова.

символ для числа n. Так, $\frac{1}{10}$ обозначалось, как ⌒. Следуя принятой нами раньше терминологии, мы будем все такие дроби называть *алгорифмическими*. Однако для обозначения $\frac{1}{2}$ вместо знака ⌒, который следовало бы ожидать, египтяне употребляли особый символ ⚌, а ⌒ означал не $\frac{1}{2}$, а $\frac{2}{3}$. Символ ⚲, который, казалось бы, должен означать единицу, на самом деле служил для обозначения $\frac{1}{3}$; $\frac{3}{4}$ в этих же записях обозначалось, как ⌒. Впоследствии ⌒ уже служило для обозначения $\frac{1}{3}$, а $\frac{3}{4}$ по общему правилу представлялось, как $\frac{1}{2}+\frac{1}{4}$. Но специальные значки для $\frac{1}{2}$ и $\frac{2}{3}$ сохранились неизменными.

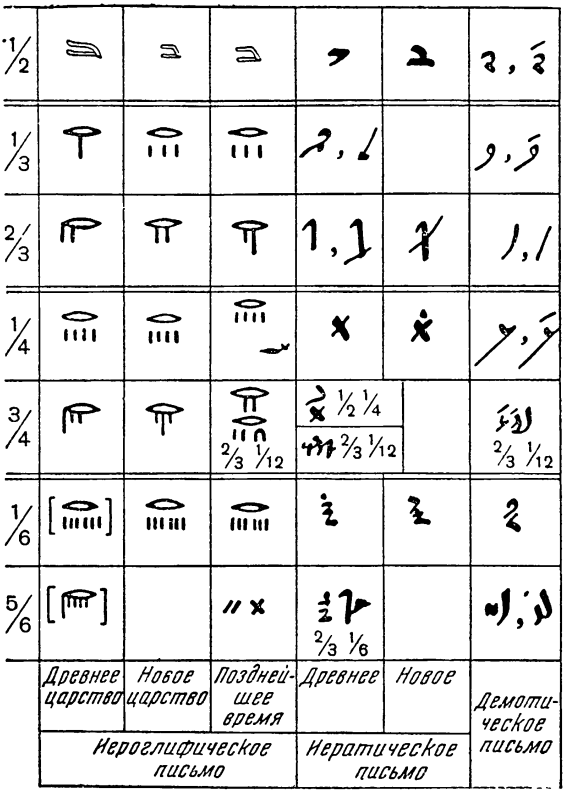


Рис. 3.

Такие же индивидуальные обозначения, отступающие от общего правила, для группы небольших дробей имелись у вавилонян (рис. 4), греков и римлян.

Так, $\frac{1}{2}$ обозначалась у греков символом $<$, тогда как все дроби $\frac{1}{n}$ при $n \geqslant 3$ обозначались символом для соответствующего числа n со штрихом справа сверху (например, γ' означало $\frac{1}{3}$, а символ β', который должен был бы обозначать $\frac{1}{2}$, обозначал $\frac{2}{3}$), т. е. картина обозначений здесь та же, что и в Египте. Аналогично этому по-аккадски для обозначения $\frac{2}{3}$ употреблялось выражение šittâ qâtâ, т. е. «обе руки», а для $\frac{3}{4}$ — šalâstâ qâtâ, т. е. «три руки». У римлян эти же дроби выражались словами bes (binae partes) и tres partes, т. е. две части и три части,

Нет ни одного языка, в котором слово для обозначения $\frac{1}{2}$ являлось бы производным от слова «два». Так, по-латыни $\frac{1}{2}$ называется semis (а два — duo), по-немецки $\frac{1}{2}$ — halb, в то время как 2 — zwei, у нас по-русски: «половина» и т. д.

Дроби	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{2}{3}$
Древнейшее, сумерийское начертание			
Позднейшее, аккадское			

Рис. 4.

Дроби, имеющие индивидуальные названия или обозначения, мы будем называть *узловыми*. Различие в обозначениях узловых и алгорифмических дробей, как мы покажем, отражает различие в их происхождении. В то время как узловые дроби возникли непосредственно из практики, как самостоятельные числовые сущности, а не как производные от целых чисел, алгорифмические дроби явились результатом последующей математической обработки.

То обстоятельство, что дроби произошли не в результате деления, подтверждается не только указанной неоднородностью дробей, но и некоторыми известными из истории примерами деления целых чисел друг на друга. Так, в одной арабской рукописи XII в. н. э. имеется задача: «разделить 100 фунтов между одиннадцатью человеками поровну». Автор решения получает при делении остаток, равный 1 фунту. Для его распределения автор не прибегает к дробям — он предлагает променять этот фунт на яйца, которых, как он устанавливает, придётся 91 штука. Распределив 88 яиц по 8 на каждого человека, автор предлагает оставшиеся три яйца отдать за труды тому, кто делил, или же променять их на соль к яйцам. Подобным же образом поступает учёный Одо Клюнийский (ум. 942 или 943). Деля 1001 фунт на 100, он раздробляет полученную в остатке единицу в унции, драхмы и т. д., пока число долей не станет больше ста. Так как и после этого деление нацело невозможно, он предлагает получившийся маленький остаток совсем отбросить. Деление здесь не приводило, таким образом, к дробям, но осуществлялось путём введения более мелких именованных единиц, а незначительный остаток просто отбрасывался.

Для выяснения вопроса о происхождении дробей нужно обратиться не к счёту, а к другому процессу, появившемуся с самых древних времён наряду со счётом, — к измерению. Исторически дроби возникли в процессе измерения. В основе всякого измерения

всегда лежит некоторая область величин (длины, объёмы, веса и т. д.). Выбор той или иной единицы, служащей основанием системы мер, обусловливается конкретной исторической обстановкой.

Меры в своём развитии прошли примерно те же этапы, что и числа.

На первых стадиях развития человеческого общества измерение производилось «на-глаз». Мера воспринималась как некоторое свойство предмета, т. е. и здесь первоначально можно говорить лишь о мере — качестве. С дальнейшим развитием общества, когда такое измерение «на-глазок» стало явно недостаточным, появились некоторые натуральные меры, которыми были прежде всего, части человеческого тела: длина ступни, ширина ладони, расстояние от локтя до конца вытянутого среднего пальца и т. д.

О существовании таких древнейших мер говорит название мер длины, сохранившееся вплоть до наших дней. Такими мерами являются фут (длина ступни), дюйм (ширина большого пальца руки при его основании), ярд (локоть), пальма (ширина ладони). К этой же категории мер относятся маховая сажень (расстояние между средними пальцами разведённых рук) и косая сажень (расстояние между большим пальцем левой ноги, широко отодвинутой от правой, и средним пальцем вытянутой вверх правой руки), бывшие долгое время в употреблении у нас в России. Меры эти служили первоначально для установления равенства измеряемых величин (равновеликости), а также для установления того, какое кратное некоторой единицы меры содержится в измеряемой величине. При этом единицу меры E повторяли целое число раз, до тех пор пока её кратное $nE = E + \ldots + E$ не становилось примерно равным измеряемой величине A $\left(\text{т. е. пока } |A - nE| < \frac{1}{2}E\right)$. Этим устанавливалась связь измерения со счётом. Потребности более точного измерения привели к тому, что первоначальные единицы мер стали раздроблять на две, три или четыре части. Получившаяся в результате раздробления более мелкая единица меры получала индивидуальное название, и величины измерялись уже в этой, более мелкой единице.

Таким образом возникали первые конкретные дроби как определённые части некоторых определённых мер. Лишь много позднее названия этих конкретных дробей стали служить для обозначения таких же частей других величин, а затем и для отвлечённых дробей.

«Не следует путать „четверть“ и „четь“, как единицу измерения земельной площади или меры сыпучих тел, с „четвертью“ или „четью“, как дробью», — пишет Л. В. Черепнин[1]). Долгое время выражение «полчетверти» означало $\frac{1}{8}$, но половина четверти как

[1]) Л. В. Черепнин, Русская метрология, М., 1944, стр. 53.

земельной меры обозначалась словом осьмина, употреблявшимся только как определённая земельная мера. Нельзя было сказать, например, осьмина книги или осьмина пути. Только много позднее осьмина стала служить для обозначения дроби $\frac{1}{8}$. Аналогично этому унция в римской системе мер первоначально означала $\frac{1}{12}$ часть денежной — весовой единицы асс. Однако постепенно слово унция начали употреблять как двенадцатую часть любой величины, т. е. в смысле отвлечённой дроби, и стало возможным говорить о пяти унциях пути или семи унциях книги.

Итак, первоначально узловые дроби служили названием определённых частей некоторых определённых мер. Отвлечённых дробей в это время ещё не существовало.

Это утверждение полностью подтверждается рассмотрением тех символов, которые первоначально употреблялись для обозначения индивидуальных дробей. Вавилонские символы для $\frac{1}{2}$, $\frac{1}{3}$ и $\frac{2}{3}$ являлись одновременно изображениями сосудов, т. е. конкретных мер объёма. Египетской единицей площади был сетат — квадрат со стороной в один хет (один хет равен 100 локтям). Четверть сетата называлась «ломаной» и обозначалась . Впоследствии слово «ломаная» стало общим названием дробей, а символ начал обозначать в иератической системе отвлечённую дробь $\frac{1}{4}$. Есть основание предполагать, что половина сетата обозначалась знаком (или). Единицей объёма служил «гекат», равный приблизительно $4\frac{1}{2}$ *л*. Так как эта единица была очень мала, то обычно в качестве единицы принимали 100 гекатов. Половина и четверть этой единицы обозначались также при помощи символов и , поставленных под символом, изображающим 100 гекатов [1]).

Обозначение типа Г, где буквой Г мы условно обозначили символ геката, полностью аналогично употреблявшемуся римлянами выражению 5 унций пути. Такое перенесение названий определённой части одной меры для обозначений той же части другой меры явилось важнейшим шагом на пути создания абстрактного понятия дроби.

Другой единицей объёма у египтян было хену, равное $\frac{1}{10}$ гекатa; $\frac{1}{32}$ хену называлась частью и обозначалась символом . Впоследствии, как мы видели, этот символ употреблялся для обозначения части вообще.

---

[1]) И. Н. Веселовский, Египетская наука в Греции, стр. 437—440. Труды Института истории естествознания, т. II, 1948.

Таким образом, знаки для узловых дробей были первоначально знаками конкретных единиц мер. Затем эти знаки, написанные в сочетании с другими единицами мер, стали обозначать доли этих других единиц. То общее, что имеют определённые доли различных мер — дробь, выделялось постепенно. Далеко не сразу было замечено, что арифметические свойства дробей, получаемых первоначально путём повторения m раз n-й доли некоторой величины x: $\overline{x} = \frac{m}{n} x$, не зависят от свойств той области величин, к которой принадлежит x. Процесс шёл много медленнее, чем процесс образования отвлечённого целого числа. Достаточно сказать, что даже римляне пользовались только конкретными дробями.

Есть все основания предполагать, что первоначально существовали только двоичные дроби. «Первой дробью, с которой познакомилось человечество, как нетрудно видеть а приори, была половина в её строго конкретной форме, именно в виде половины какого-нибудь реального предмета» [1]).

Вслед за половиной появляются дроби, идущие по двоичной системе. Этот этап развития нашёл своё выражение в древнеегипетской метрологии. Единицу площади сетат египтяне подразделяли на вторые, четвёртые, восьмые, шестнадцатые и тридцать вторые доли. Такие же подразделения имела и мера объёма — гекат. Для всех этих долей существовали индивидуальные названия. «В силу конкретности этих долей счёт их производился так же, как и счёт всяких целых предметов» [2]). Естественно, что числителями таких дробей могли быть только единицы. Позднее к этим дробям была присоединена $\frac{1}{3}$ и её двоичные подразделения. Такие подразделения встречаются в более позднем египетском способе деления (образование половинного и двух-третних рядов). Подобным же образом строились и древнерусские меры. Так, единицей земельно-податной меры являлась соха, которая делилась на «полсохи», «треть сохи», «четверть сохи», «полтреть сохи», «пол-полтреть сохи» и «пол-пол-полтреть сохи». Другой земельной мерой была четверть, от которой бралась сначала треть, а потом половинные доли, наименьшей из которых была «пол-пол-пол-пол-пол-пол-пол-пол-пол-пол-полтретних».

Система древнерусских дробей строилась по тому же принципу, что и система мер. Основными дробями являлись:

$\frac{1}{2}$ числа, которая обозначалась словом «пол»,

$\frac{1}{3}$ » » » » «треть»,

---

[1]) В. В. Бобынин, Отзыв о сочинениях Н. М. Бубнова, стр. 114.
[2]) В. В. Бобынин, Цит. соч., стр. 115.

$\frac{1}{4}$ числа, которая обозначалась словом «четь, или четверть»,
$\frac{1}{6}$ » » » » «полтрети»,
$\frac{1}{8}$ » » » » «полчети», или «полчетверти»,
$\frac{1}{12}$ » » » » «пол-полтрети»,
$\frac{1}{16}$ » » » » «пол-полчети»,
$\frac{1}{24}$ » » » » «пол-пол-полтрети», или «малые трети»,
$\frac{1}{32}$ » » » » «пол-пол-полчети», или «малые чети».

Остальные дроби в древнерусских источниках часто выражались посредством сложения и вычитания этих «основных» дробей. Так $\frac{11}{24}$ схематически представлялось как $\frac{1}{3}+\frac{1}{12}+\frac{1}{24}$; $\frac{29}{96}=\frac{1}{3}-\frac{1}{32}$.

Все эти соотношения выражались словами. Для обозначения какого-нибудь числа единиц без половины единицы употреблялось выражение «пол» этого неполного числа единиц. Так, $2\frac{1}{2}$ называлось «полтретьи», $3\frac{1}{2}$ — «полчетверти», $4\frac{1}{2}$ — «полпяты», $5\frac{1}{2}$ — «полшесты» и т. д. В качестве пережитка у нас до сих пор сохранилось выражение «полтора» для $1\frac{1}{2}$, т. е. «полвтора» — полвторого. Аналогичная система обозначения сохранилась у нас при счёте времени (полпятого, полшестого и т. д.)[1]).

По гипотезе И. Н. Веселовского египтяне от двоичных дробей перешли к дробям вида $\frac{1}{n}$ в связи со счётом времени. При этом в качестве «числителя» дроби продолжали фигурировать только единицы. Число $\frac{15}{17}$, например, не могло быть выражено в египетской системе при помощи единого символа. Понятие о $\frac{15}{17}$, как о едином числе, единой дроби, у египтян не было. Все дроби вида $\frac{m}{n}$, где $m>1$, они представляли по общим правилам в виде суммы $\sum_i \frac{1}{n_i}$, причём $n_i \neq n_j$, если $i \neq j$. Так как число m можно пред-

[1]) Подобные же образования сохранились и в датском языке. Так 50 по-датски halvtresindstyve, что означает буквально полтри раза по двадцать.

ставить в двоичной системе $m = 2^{n_1} + 2^{n_2} + \ldots + 2^{n_k}$, $n_1 > n_2 > \ldots > n_k \geqslant 0$, то для представления $\frac{m}{n}$ в виде суммы $\sum \frac{1}{n_i}$ достаточно было уметь представлять в таком виде дроби $\frac{2}{n}$. И действительно, в египетских папирусах мы находим таблицы для подобного разложения $\frac{2}{n}$, $n = 3, 5, \ldots, 101$. О том, как были составлены эти таблицы, существует много различных гипотез, которых мы здесь касаться не будем[1]). Отметим только, что уже при составлении этих таблиц, преследовавших чисто практические цели, египетскому вычислителю пришлось столкнуться с теоретико-числовыми проблемами.

В Греции, так же как и в Египте, употреблялись по преимуществу дроби вида $\frac{1}{n}$. Видимо, первоначально этой областью греческие дроби и ограничивались. Для обозначения дроби $\frac{1}{n}$, как мы говорили, писалось числовое значение n со штрихом справа. Так $\frac{1}{23}$ записывалась, как $\kappa\gamma'$ ($\kappa = 20$, $\gamma = 3$).

Герон Александрийский (I—II вв. н. э.) употреблял дроби вида $\frac{m}{n}$. Для их обозначения он сначала писал символ для m со штрихом справа, а затем дважды повторял символ для n, снабжённый двумя штрихами справа. Например, дробь $\frac{2}{5}$ обозначалась, как $\beta'\varepsilon''\varepsilon''$, а дробь $\frac{23}{33}$, как $\kappa\gamma'\lambda\gamma''\lambda\gamma''$ ($\kappa = 20$, $\lambda = 30$, $\gamma = 3$).

Диофант (III в. н. э.) обозначал дробь, как и мы, при помощи черты, только знаменатель он записывал над чертой, а числитель — под ней. Так, дробь $\frac{21}{25}$ он записывал в виде $\frac{\kappa\varepsilon}{\kappa\alpha}$ ($\kappa\varepsilon = 25$, $\kappa\alpha = 21$). Дробь $\frac{1\,270\,538}{10\,817}$ выглядела так: $\frac{\alpha,\omega\iota\zeta}{\rho\kappa\zeta\cdot\varphi\xi\eta}$.

У Диофанта встречается и другое обозначение дробей: сначала записывается числитель, затем знаменатель, между которыми пишется слово μοριον (частица). Например:

$$\frac{3\,069\,000}{331\,776} = \overline{\tau\varsigma}\cdot\ ,\bar{\theta}\mu o\rho\cdot\overline{\lambda\gamma}\cdot\ ,\overline{\alpha\psi o\varsigma}.$$

Так же как и в Египте, в Греции было распространено представление дробей в виде суммы дробей с числителями единица. Например, $\frac{9}{20} = \frac{1}{4} + \frac{1}{5} = \delta'\varepsilon'$ (сложение заменялось простым приписыванием).

---

[1]) См. цитированную выше статью И. Н. Веселовского и статью С. А. Яновской «К теории египетских дробей». Труды Ин-та истории естествознания, т. I, 1947.

Для астрономических расчётов греки употребляли вавилонские шестидесятиричные дроби, о которых мы скажем ниже.

Как уже говорилось, в отличие от греков римляне пользовались только конкретными дробями, а именно частями денежной единицы асс, подразделявшейся на 12 унций. Впоследствии унции стали применяться для измерения любой величины. Таким образом, Рим, знавший только именованные дроби, отставал в этом отношении даже от Египта более чем на полторы тысячи лет. Знаком для унции служила черта —, половина обозначалась буквой S (первая буква слова semis). Остальные двенадцатиричные дроби выражались комбинацией этих двух символов.

Например, $\frac{7}{12}=\frac{6}{12}+\frac{1}{12}=\frac{1}{2}+\frac{1}{12}=$ S —,

$\frac{1}{24}$ асса называлась семунцией (semunzia),

$\frac{1}{36}$ » » дуэллой (duella),

$\frac{1}{48}$ » » сициликом (sicilicus),

$\frac{1}{72}$ » » секстулой (sextula).

Второй ряд подразделений основной единицы шёл следующим образом: $1=$ асс, $\frac{1}{12}=$ unzia, $\frac{1}{24}=$ semunzia, $\frac{1}{288}=$ scrupel, $\frac{1}{576}=$ $=$ simplium, т. е. каждая следующая дробь возникала из предшествующей попеременным умножением знаменателя на 2 и на 12. Весовая единица асс и её подразделения на унции долгое время сохранялись в аптекарском обиходе. Двенадцатиричные дроби римлян долгое время были в употреблении и у средневековых абацистов. На примере истории римских дробей можно видеть «непосредственное применение метрологической системы, выработанных для неё правил и приёмов счисления к отвлечённым дробям и выполнению над ними действий счёта» [1]). Такие случаи наблюдались и в других местах.

Индусы не распространили изобретённую ими десятичную позиционную систему на изображение дробей. Простые дроби они обозначали, надписывая числитель над знаменателем, но не ставили разделительной черты. Так, в Бахшалинской рукописи дробь $\frac{1}{3}$ изображается, как $\frac{1}{3}$. При изображении смешанной дроби целая часть надписывалась над числителем. Например, число $1\frac{1}{3}$ схематически изображалось, как $\frac{1}{1\,3}$. Такая запись впервые встречается у

[1]) В. В. Бобынин, Отзыв о сочинениях Н. М. Бубнова, стр. 119.

таджикского учёного ал-Насави (ум. ок. 1030 г. н. э.), причём в случае отсутствия целой части ал-Насави приписывал сверху нуль; $\frac{1}{11}$ он изображал так $\frac{0}{1}_{11}$. Дробную черту мы встречаем у ал-Хассара (XII в.). Леонардо Пизанский применял её регулярно. Однако общеупотребительной она стала только в XVI в. Символы для изображения дроби в средние века были крайне разнообразны. Иногда числитель и знаменатель записывали при помощи римских цифр, своеобразно используя мультипликативный принцип. Так, в одной немецкой книге по арифметике (1514) дробь $\frac{200}{460}$ изображалась, как $\frac{\text{II}^{\text{C}}}{\text{IIII}^{\text{C}}\text{LX}}$. В манускрипте середины XIV в. встречаются обозначения $3\bar{5}$ для $\frac{3}{5}$ и $4\bar{7}$ для $\frac{4}{7}$. Часто вместо $\frac{1}{2}$ писали $\div$; так $4\div$ означало $4\frac{1}{2}$. При произношении дроби в средние века всегда добавляли слово «части»: $\frac{2}{5}$ произносилось, как две пятых части.

В России (XVI—XVII вв.) при выговаривании дроби со знаменателем от 5 до 10 прибавляли окончание «ина». Например, $\frac{1}{7}$ — седьмина, $\frac{1}{10}$ — десятина. Если знаменатель был более десяти, то к названию дроби добавлялось слово «жеребей». $\frac{5}{13}$, например, читалось, как пять тринадцатых жеребьев. Дроби в русских рукописях назывались долями; позднее их стали именовать ломаными числами, что соответствовало латинскому термину numeri fracti. Такой терминологии придерживался и Магницкий в своей «Арифметике».

Единообразное алгорифмическое представление любых дробей впервые было проведено вавилонянами, обозначавшими дроби по той же шестидесятиричной позиционной системе, что и целые числа. При таком обозначении дроби подразумевалось известным, какие именно доли единицы берутся (60-е, 3600-е и т. д.); в записи непосредственно отмечалось только количество взятых долей. Индивидуальные обозначения небольшой группы дробей $\left(\frac{1}{2}, \frac{1}{3}, \frac{2}{3}\right.$ и т. д.$\left.\right)$ были почти полностью вытеснены из математических текстов. Даже $\frac{1}{2}$ впервые получила тут алгорифмическое представление в виде ⟨⟨ (0,30). Шестидесятиричные дроби имели то неоспоримое преимущество, что оперировать с ними можно было по тем же правилам, что и с целыми числами. Благодаря этому шестидесятиричные дроби позднее распространились за пределы Вавилона.

Вероятно, не позднее середины II в. до н. э. дроби эти главным образом через посредство астрономических сочинений перешли в Александрию. Так как греческая алфавитная система нумерации была мало приспособлена для записи больших чисел и для оперирования с ними, то астрономам для вычислений таблиц нужно было либо ввести новую систему нумерации для целых чисел и принять радиус окружности равным достаточно большому целому числу (тогда хорды выражаются с нужной степенью точности в целых единицах этого радиуса), либо ввести новый способ представления дробей. Греческие астрономы выбрали последнее. Они оставили неизменной нумерацию целых чисел, а для дробей применили шестидесятиричную систему вавилонян, в которой они только изменили начертание цифр. Числа от 1 до 59 они обозначали не по аддитивному принципу при помощи знаков ❜ и ❛, а при помощи букв алфавита.

Знаменитый греческий астроном Клавдий Птолемей (II в. н. э.) делил окружность круга на 360 частей. Для этих частей Птолемей иногда употреблял слово τμήματα, т.е. о т р е з к и, которое было дословно переведено латинским словом segmentes. Чаще он называл их просто частями: μοῖραι, сокращённо обозначая их μ°. Впоследствии начали писать один только верхний кружок, который сохранился до сих пор для обозначения градуса. Само слово «градус», по мнению Г. Нессельмана (1842), имеет арабское происхождение.

Каждую из получившихся частей (градусов) Птолемей делил в свою очередь на 60 частей, которые он называл словом λεπτα, дословно означающим «мелочь», или «первыми шестидесятыми». Следующие два шестидесятиричные подразделения он называл «вторыми шестидесятыми» и «третьими шестидесятыми». При переводе на латынь эти подразделения получили названия: minuta prima, minuta secunda, minuta tertia (т. е. первая минута, вторая минута и третья минута); слово «minuta» означает «уменьшенная» или «мелкая», являясь, таким образом, латинским переводом греческого слова «λεπτα». Отсюда произошли наши слова минута и секунда. Птолемей пользовался обычно не полными, а сокращёнными обозначениями шестидесятиричных разрядов, при этом его обозначение минут, секунд и терций совпадало с современным. Число 37°4′55″ он записывал, как μ°λζδ′νε″. Иногда символ μ° опускался, и тогда над числом градусов ставилась горизонтальная черта. При записи шестидесятиричных дробей греки употребляли символ ο для обозначения пропущенного разряда, сходный по форме с нашим нулём. Так, число 12°0′24″ записывалось, как ιβ̄ο′χδ″ Целые числа продолжали записывать по обычной алфавитной системе. Буква ο являлась в ней, как и прежде, символом для числа 70. В записи шестидесятиричных дробей число 70 встретиться не могло (так как число единиц в каждом шестидесятиричном разряде не превосходит 59), поэтому

букве о (омикрон) можно было приписать новое числовое значение. Предполагают, что знак 0 возник в результате сокращения слова οὐδέν — ничего.

Заметим, что при специальном обозначении разрядов такой символ вовсе не был необходим, в то время как в вавилонской системе, когда отдельные разряды никак не отмечались при записи, введение межразрядового символа было очень существенным.

Шестидесятиричные дроби перешли от вавилонян не только к грекам, но и в страны Среднего и Ближнего Востока, а затем и в Западную Европу. Дроби эти употреблялись только в научных сочинениях; в общежитие они не вошли. В Средние века, таким образом, в Европе для представления целых чисел употреблялась десятичная позиционная система нумерации, а для дробей — либо шестидесятиричная система, либо различные представления в виде простых дробей [1]).

Некоторые намёки на десятичные дроби встречались ещё у индусов, которые при извлечении квадратного корня, в случае, если он не извлекался нацело, приписывали к подкоренному выражению столько пар нулей, сколько нужно было получить лишних знаков в корне. Однако десятичные дроби индусы всегда писали со знаменателем и не распространяли на них общей десятичной нумерации. Аналогичные приёмы употребляли и математики Среднего Востока, например ал-Насави.

В Европе подобный способ извлечения квадратных корней был впервые применён Иоанном Севильским в упоминавшемся уже нами сочинении «Практическая арифметика алгоризма» (XII в. н. э.). В середине XV в. при составлении тригонометрических таблиц учёные иногда принимали радиус круга равным 10^6 или 10^7 (Региомонтан и др.) и, таким образом, фактически получали значения тригонометрических величин в десятичных дробях.

В XV — XVI вв. дроби с десятичными знаменателями встречаются всё чаще. Так, мы находим довольно развитое учение о дробях с десятичными знаменателями у одного математика XIV в., жившего во Франции [2]). Подобные же дроби встречаются и у Кардана (XVI в.) [3]). Немецкий арифметик Грамматеус (1523)

[1]) Действия с дробями долгое время считались труднейшим и запутаннейшим отделом арифметики. У немцев до сих пор сохранилась поговорка — «попасть в дроби» (in die Brüche gerathen), употребляемая в смысле «попасть в тупик». Глава о дробях помещалась обычно в самом конце учебника, чтобы учащийся, не желающий себя слишком затруднять, мог овладеть остальными правилами арифметики без знания дробей. Большинство учеников так до этой главы и не добиралось.

[2]) О нём см.: Gandz, The invention of the decimal fractions and application of the exponential calculus by Immanuel Bonfils of Tarascon (Isis, XXV (1), 1936).

[3]) Самаркандский математик и астроном Джиат-Эддин Джемшид ал-Каши около 1420 г. выразил в виде десятичной дроби более чем с 15 знаками отношение длины окружности к радиусу.

советовал применять такие дроби для сравнения простых дробей. Чтобы узнать, какая из дробей $\frac{5}{8}$ и $\frac{2}{3}$ больше, он приписывал к каждому из числителей нули, т. е. раздроблял их в десятичные доли, а затем делил их на знаменатели: $\frac{500}{8}=62\frac{1}{2}$ и $\frac{200}{3}=66\frac{2}{3}$, откуда $\frac{2}{3}>\frac{5}{8}$.

Французский учёный Оронс Финэ (примерно 1550) при извлечении квадратного корня из 10 приписал к 10 шесть нулей, также получив фактически выражение искомого корня в десятичных дробях. Однако он сразу же перевёл полученное выражение в привычные шестидесятиричные дроби. Этот пример ясно показывает, что, несмотря на фактическое появление десятичных дробей, вплоть до последней четверти XVI в. они не применялись сколько-нибудь систематически.

Впервые начал последовательно применять десятичные дроби фламандский инженер и учёный Симон Стевин (1548—1620). В 1584 г. он издал на фламандском языке, а вскоре после этого и на французском таблицу процентов, а в следующем году опубликовал сочинение «La disme enseignant facilement expédier par nombres entiers sans rompuz tous comptes se rencontrans aux affaires des hommes» («Десятая, обучающая легко производить все расчёты, встречающиеся в людских делах, с помощью целых чисел, без дробей»). В этой брошюре, содержавшей всего семь страниц, и были введены десятичные дроби. Стевин вполне понимал значение десятичных дробей и распространил на них все действия арифметики. Он видел, что десятичные дроби были бы особенно полезны при условии введения десятичной системы мер, первым энергичным поборником которой он и сделался. Его желанием как можно шире распространить десятичную систему объясняется и то, что он написал «La disme» не по-латыни, а на разговорных фламандском и французском языках.

Обозначение десятичных дробей, предложенное Стевином, значительно отличалось от современного. Вместо нашей запятой он употреблял нуль, заключённый в кружок, а после каждого десятичного разряда указывался его порядковый номер, который также помещался в кружок. Например, число 35,912 записывалось им так: 35⓪9①1②2③. В этом способе записи применяется тот же принцип, что и в предложенном Стевином обозначении показателей степеней неизвестных.

В 1608 г. «La disme» была переведена на английский язык Ричардом Нортоном, а в 1619 г. в Англии было опубликовано сочинение Генри Ляйта по десятичной арифметике.

Однако десятичные дроби далеко не сразу вытеснили все остальные. Им, как и десятичной позиционной системе счисления,

пришлось с трудом пробивать себе дорогу, завоёвывая себе место в упорной борьбе со старой традицией.

На континенте после Стевина десятичные дроби систематически применял Бюрги (1552—1632), швейцарец по рождению, рукописные сочинения которого относятся примерно к 1592 г. Бюрги употребил в качестве знака отделения целой части числа от дробной нуль, поставленный над цифрой для единиц.

В 1603 г Бейер во Франкфурте-на-Майне выпустил сочинение «Logistica Decimalis» («Десятичная арифметика»), в котором излагал правила действия с десятичными дробями. Эти дроби Бейер считал своим собственным изобретением. Бейерово обозначение десятичных дробей напоминает господствовавшее в то время обозначение для шестидесятиричных дробей. Число 123,459872 он записывал в виде
0 I II III IV V VI 0 III VI VI
12 3-4-5-9-8-7-2 или короче в виде 123-459-872. Число 54 означало в его системе 0,000054. Бейер замечает, что его дроби отличаются от обычных тем, что при их обозначении знаменатель надписывается над числителем.

В течение XVI—XVII вв. продолжали существовать различные обозначения для десятичных дробей.

Первое введение в качестве разделительного знака запятой приписывается Бюрги и Кеплеру (1571—1630), употреблявшим её наряду со скобкой.

Десятичными дробями занимался и Непер (1550—1617), изложивший теорию этих дробей в своём сочинении «Rabdologia». В этой книге дроби, как правило, обозначаются тем же способом, каким мы теперь записываем градусы, минуты, секунды и т. д. Дробь 28,675 записывалась у него так: 28°6′7″5‴, что читалось, как 28 целых, 6 прим, 7 секунд, 5 терций. Иногда разряды у него разделялись ещё двумя точками. В этом же сочинении Непер применил в качестве разделительного знака точку, применяющуюся до сих пор в качестве разделительного десятичного знака в Англии и Америке [1]). Однако наряду с десятичными дробями на протяжении всего XVII в. встречаются ещё и шестидесятиричные дроби, которые были окончательно вытеснены только в XVIII в.

У нас, в России, изложение учения о десятичных дробях впервые встречается в «Арифметике» Л. Магницкого (1703). Магницкий различал арифметику — логистику или астрономскую, т. е. оперирующую с шестидесятиричными дробями, которые он записывал в виде
0 I II III IV
51 25 42 51 25, и иную арифметику, «яже децималь или десятичная именуется», которую он употреблял только в геометрии. Излагая эту десятичную арифметику, он описывает десятичные меры длины и площади. В качестве мер длины там вводилась рута (гер-

---

[1]) Впервые употреблял (не систематически) десятичную точку Хр. Клавий (1593).

манская сажень), равная 10 футам; 1 фут = 10 цолей, или пальцев; цоль = 10 гран, или зёрен; гран = 10 скрупелей, или дробей.

В XVIII в. десятичные дроби получают всё бóльшее распространение. Окончательно они укрепились в связи с введением десятичной системы мер и весов [1]). Теперь и в житейском обиходе, не говоря уже о статистике, чаще употребляют проценты (т. е. десятичные дроби), чем простые дроби.

---

[1]) Единая десятичная система мер и весов была впервые введена только после Французской буржуазной революции 1789 г. У нас, в СССР, метрическая система была введена постановлением Совнаркома от 14 января 1918 г. К 1926/27 г. она вытеснила окончательно старую систему.

Англия, США и некоторые другие страны до сих пор не ввели у себя обязательной метрической системы.

ЗАКЛЮЧЕНИЕ

С возникновением десятичных дробей десятичная позиционная система достигла завершения, приобрела необходимую для нумерации полноту и в основном стала господствовать в научном и житейском обиходе. Наряду с нею сохранились только крайне незначительные пережитки других систем, частью в речи, частью в расчётах (шестидесятиричное деление часа и градуса, применение ряда простых дробей: $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$ и т. д.), иногда при порядковой нумерации (с помощью букв алфавита).

Вместе с тем современная нумерация, которая возникла первоначально лишь для представления целых чисел, с введением десятичных дробей распространилась на все действительные числа [1]). При этом к ней не пришлось добавлять никаких существенно новых принципов; обозначение всех чисел с её помощью производится вполне единообразно.

Десятичная позиционная система, как легко видеть, полностью удовлетворяет всем требованиям, которые можно предъявить к удобной системе нумерации (см. стр. 33 настоящей статьи). Она одинаково удобна для представления и весьма больших и весьма малых чисел, которыми, начиная с эпохи Возрождения, человечеству приходится пользоваться во всё возрастающей мере и особенно в наш век исследований сверхгалактик, с одной стороны, и внутриатомного микромира, с другой. Этим требованиям в сколько-нибудь полной мере не удовлетворяла ни одна из предшествующих систем нумерации. Поэтому-то при поступательном движении человечества вперёд все они должны были уступить место десятичной позиционной системе, вопреки многовековой традиции и иным препятствиям.

Как мы видели, десятичная позиционная система явилась плодом долгого исторического развития. В создании её, растянувшемся на тысячелетия, приняли участие многочисленные народы Востока и Запада. История её происхождения представляет интерес не только в рамках одной дисциплины — математики, но имеет и более общее значение.

---

[1]) О действительных числах см. стр. 188, И. В. Проскуряков, Понятия множества, группы, кольца и поля. Теоретические основы арифметики.

1. Прежде всего подлинно научная и объективная история нумерации опровергает идеалистические учения об априорном характере понятия числа, о его мнимой прирождённости человеческому сознанию. История нумерации показывает, что понятие натурального числа (как и дроби), с его свойствами и законами возникло в результате отвлечения от определённых и вполне конкретных количественных свойств и отношений предметов реального мира, подобно тому как геометрия «...даёт свои законы, абстрагируясь от конкретных предметов, рассматривая предметы, как тела, лишённые конкретности, и определяя отношения между ними не как конкретные отношения таких-то конкретных предметов, а как отношения тел вообще, лишённые всякой конкретности» [1]).

2. Далее, история нашей нумерации показывает, что развитие систем счисления шло от разнообразия и разнородности к единству и однородности. Чем ниже был хозяйственный и культурный уровень общества, тем разнообразнее были употребляемые в нём системы счисления.

Первой всеобщей формой нумерации явились системы счисления типа иероглифической, основанные на аддитивном (а иногда и субтрактивном) принципе. Фазу иероглифической нумерации, соответствующую ещё очень примитивному устному счёту, в более или менее развитой её форме прошли, повидимому, все народы. Хотя принцип её построения в различных странах был один и тот же, но в выборе узловых чисел, каждое из которых служило основанием своей особой системы, а также в начертании их наблюдался полный разнобой.

Нумерацией нового типа, сменившей иероглифические системы, была алфавитная система счисления, явившаяся важнейшим шагом на пути создания современной универсальной нумерации. Она была хорошо приспособлена к оперированию с не очень большими числами в соответствии с хозяйственным диапазоном античной рабовладельческой формации или раннего феодализма.

Все алфавитные системы строились на общем им цифирном принципе и были десятичными. Эти два обстоятельства являлись важным шагом на пути создания единой нумерации. Однако то, что каждый народ применял при этом свой собственный алфавит, препятствовало созданию такой единой системы.

Наконец, последнюю стадию развития нумерации составляет наша десятичная позиционная система счисления, первая единообразная система, принятая во всём мире. Единым здесь является не только принцип её построения, но и начертание цифр.

3. Вместе с тем история нумерации служит дополнительной иллюстрацией сталинского положения о развитии через борьбу,

---

[1]) И. Сталин, Относительно марксизма в языкознании, Издательство «Правда», 1950, стр. 23.

борьбу нового и передового со старым и консервативным, о неодолимой и всепобеждающей силе прогрессивных элементов человеческого общества и человеческой культуры. Действительно, всякая система нумерации фиксирует уже существующий устный счёт. Счёт этот продолжает развиваться и совершенствоваться вместе с дальнейшим прогрессом общества. При этом зафиксированная в символах система счисления часто отстаёт от фактически существующих способов счёта. Тогда с неизбежностью появляются новые, более совершенные системы счисления. Мы видели, с каким трудом приходилось им всякий раз пробивать себе дорогу. Так, алфавитной системе пришлось преодолевать вековую традицию аттических государств, а десятичной позиционной системе противостояли реакционные силы европейского средневековья.

4. Наконец, история происхождения позиционной системы вновь показывает единство законов общественного развития. Подходом к позиционному принципу, как мы видели, служили мультипликативные системы, которые привели к созданию позиционности и введению нуля в Древнем Двуречье, у племени Майя, в позднеантичную эпоху и, наконец, в Индии. Создание современной позиционной системы не было, таким образом, случайным, а явилось закономерным завершением неизбежного исторического процесса.

История нумерации во многом сходна с историей языков, о которой И. В Сталин пишет: «Язык порождён не тем или иным базисом, старым или новым базисом, внутри данного общества, а всем ходом истории общества и истории базисов в течение веков. Он создан не одним каким-нибудь классом, а всем обществом, всеми классами общества, усилиями сотен поколений. Он создан для удовлетворения нужд не одного какого-либо класса, а всего общества, всех классов общества. Именно поэтому он создан, как единый для общества и общий для всех членов общества общенародный язык. Ввиду этого служебная роль языка, как средства общения людей, состоит не в том, чтобы обслуживать один класс в ущерб другим классам, а в том, чтобы одинаково обслуживать всё общество, все классы общества» [1]). История систем счисления показывает, что наша нумерация также была создана всем ходом истории общества и истории базисов в течение веков, усилиями сотен поколений и создана для обслуживания всего общества, всех его классов как система, единая для общества и общая для всех его членов.

---

[1]) И. Сталин, Относительно марксизма в языкознании, Издательство «Правда», 1950, стр. 5—6.

И. В. ПРОСКУРЯКОВ

ПОНЯТИЯ МНОЖЕСТВА, ГРУППЫ, КОЛЬЦА И ПОЛЯ. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АРИФМЕТИКИ

*

ВВЕДЕНИЕ

Понятие числа, возникшее на самых ранних ступенях развития человеческого общества из потребностей счёта, является одним из основных завоеваний человеческой культуры. Число является постоянным и незаменимым орудием всей нашей практической деятельности. Возможность применять числа для изучения и изменения окружающего нас материального мира обусловлена тем, что сами числа взяты человеком из этого мира, и все свойства чисел являются лишь абстрактным (освобождённым от ряда частных конкретных признаков) выражением реальных отношений материального мира. Так, число пять является лишь отражением в нашем уме реального свойства, общего пяти пальцам руки, цветку о пяти лепестках и всем прочим пятёркам материальных предметов независимо от их формы, размера, цвета и других конкретных свойств.

Энгельс об этом пишет: «...совершенно неверно, будто в чистой математике разум имеет дело только с продуктами собственного творчества и воображения. Понятия числа и фигуры взяты не откуда-нибудь, а только из действительного мира. Десять пальцев, на которых люди учились считать, т. е. производить первую арифметическую операцию, представляют собой всё, что угодно, только не продукт свободного творчества разума. Чтобы считать, надо иметь не только предметы, подлежащие счёту, но обладать уже способностью отвлекаться при рассматривании этих предметов от всех прочих их свойств, кроме числа, а эта способность есть результат долгого, опирающегося на опыт, исторического развития» [1]).

Такова суть математики с точки зрения диалектического материализма.

Противоположные взгляды высказываются буржуазными учёными-идеалистами. По их мнению, математика — продукт свободного творчества человеческого духа, а её основные понятия присущи нашему разуму априорно, т. е. до всякого опыта, даны человеку уже при его рождении.

Вздорность подобного взгляда на математику доказывается миллионы раз и на каждом шагу всей нашей практической деятель-

---

[1]) Ф. Энгельс, Анти-Дюринг, Госполитиздат, 1948, стр. 36—37.

ностью, когда применение математики даёт ожидаемые нами результаты. Последнее возможно только потому, что математические истины являются лишь отражением объективных закономерностей природы.

Число является основным орудием, при помощи которого математика изучает закономерности реального мира. Современное понятие о числе явилось результатом сложного и длительного процесса исторического развития. После натуральных чисел появились числа дробные, затем иррациональные и, наконец, отрицательные, комплексные. Настоящая статья лишь в самых общих чертах касается истории развития понятия числа, ставя своей задачей выяснение логической сущности этого понятия в его современном виде. Читатель не найдёт здесь большого числа новых для него свойств чисел. Не знакомство с новыми свойствами, а обоснование свойств чисел, известных каждому со школьной скамьи, — главная цель данной статьи.

Доказательство даже самых простых свойств чисел, как, например, переместительного или сочетательного закона сложения, требует точного определения числа и встречает поэтому значительные трудности. Тем не менее нам кажется, что учителю, ежедневно говорящему учащимся об этих свойствах чисел, нужно самому иметь представление о том, как они доказываются. Это весьма полезно с точки зрения развития общей математической культуры и для наиболее одарённых и интересующихся математикой школьников старших классов. По тем же соображениям статью можно рекомендовать студентам педагогических институтов. Так как построение действительных чисел входит в курс математического анализа, а комплексных чисел — в курс высшей алгебры физико-математических факультетов университетов, то соответствующие главы статьи можно рекомендовать студентам указанных факультетов.

Кроме обоснования свойств чисел, второй целью статьи является введение читателя в круг основных идей и понятий современной математики. К числу таких идей принадлежит представление об изоморфизме, а к числу понятий — понятия о множестве, группе, кольце и поле. Применение указанных общих понятий позволяет избежать многократного и утомительного повторения одних и тех же рассуждений при доказательстве аналогичных свойств чисел той или иной природы и позволяет читателю охватить свойства различных числовых областей с общей точки зрения. Конечно, у читателя, не знакомого с этими понятиями, такое изложение вызовет дополнительные трудности, так как этому новому взгляду на числа ему придётся действительно учиться. Ознакомление с этими идеями и понятиями современной математики представляет значительную часть того нового, что узнает читатель из настоящей статьи. Изложение обоснования понятия числа с точки зрения теории колец и полей может, как нам кажется, заинтересовать также и специалиста.

В главе первой даны необходимые сведения из теории множеств. В главе второй рассматриваются понятия группы, кольца и поля, причём в общем виде изучаются свойства алгебраических операций, которые затем многократно применяются при изучении чисел той или иной природы. В дальнейших главах последовательно вводятся натуральные, целые, рациональные, действительные и комплексные числа. В последнем параграфе рассматриваются также кватернионы и разбирается вопрос о возможности дальнейшего расширения числовых областей.

Имея в виду логическое обоснование свойств чисел, мы при использовании уже доказанных свойств обычно даём в скобках ссылку на соответствующую теорему из предыдущих глав. Поэтому читателю, желающему проверить правильность обоснования данного свойства, нужно либо читать всю предшествующую часть статьи, либо те части её, которые указаны в этих ссылках. Однако читателю, специально интересующемуся обоснованием свойств чисел данной природы и желающему принять свойства предыдущих числовых областей как известные, можно после первых двух глав и § 19 главы IV, где вводятся понятия, необходимые для понимания всего дальнейшего, читать сразу интересующую его главу. При таком чтении можно просто не обращать внимания на ссылки в скобках, так как свойства чисел, о которых идёт речь, сами по себе известны каждому школьнику. Так, приняв известными свойства рациональных чисел, можно после первых двух глав и § 19 читать сразу главу VI о действительных числах, приняв же известными свойства действительных чисел, можно читать главу VII о комплексных числах.

ГЛАВА I

МНОЖЕСТВА

§ 1. Понятие о множестве

Любая область математики изучает те или иные объекты не каждый в отдельности, а в их совокупности. Объекты, обладающие теми или иными общими свойствами, объединяются вместе в одну совокупность и изучаются совместно.

Совокупность всех натуральных чисел включается в более широкую совокупность целых чисел. Расширяя уже полученную числовую область, мы приходим, далее, к рациональным, действительным и, наконец, комплексным числам. В алгебре рассматриваются такие совокупности, как многочлены и алгебраические дроби. В геометрии, изучая свойства треугольника, отвлекаются от его положения на плоскости или даже от его размеров, получая теоремы, справедливые для всех равных или же всех подобных треугольников; в других случаях рассматриваются совокупности точек, обладающих тем или иным общим свойством (геометрические места) и т. д.

Мы ограничимся здесь лишь начальными сведениями из теории множеств, отсылая читателя, желающего детально с ней ознакомиться, к книгам П. С. Александрова [1] и Н. Н. Лузина [2].

Множество — это совокупность объектов, рассматриваемая как одно целое. Эти слова не следует принимать за определение понятия множества, ибо чем слово «совокупность» лучше слова «множество»? Понятие множества принимается за основное, т. е. не сводимое к другим понятиям. Объекты, составляющие данное множество, называются его *элементами*. Основное отношение между элементом a и содержащим его множеством A обозначается так: $a \in A$ (словами: a есть элемент множества A; или a принадлежит A, или A содержит a). Если a не является элементом множества A, то пишут $a \overline{\in} A$ (словами: a не входит в A, A не содержит a). Множество можно задать указанием всех его элементов, причём в этом случае употребляются фигурные скобки. Так $\{a, b, c\}$ обозначает множество трёх элементов. Аналогичная запись употребляется и в

случае бесконечных множеств, причём невыписанные элементы заменяются многоточием. Так, множество натуральных чисел обозначается $\{1, 2, 3, \ldots\}$, а множество чётных чисел $\{2, 4, 6, \ldots\}$, причём под многоточием в первом случае подразумеваются все натуральные числа, а во втором — только чётные.

Два множества A и B называются *равными,* если они состоят из одних и тех же элементов, т. е. если каждый элемент множества A принадлежит B и, обратно, каждый элемент B принадлежит A. Тогда пишут $A=B$. Таким образом, множество однозначно определяется его элементами и не зависит от порядка записи этих элементов. Например, множество из трёх элементов a, b, c допускает шесть видов записи:

$$\{a, b, c\}=\{a, c, b\}=\{b, a, c\}=\{b, c, a\}=\{c, a, b\}=\{c, b, a\}.$$

Из соображений формального удобства вводят ещё так называемое «*пустое множество*», а именно, «множество», не содержащее ни одного элемента. Мы будем обозначать его символом 0 (совпадение с обозначением числа нуль не ведёт к путанице, так как смысл символа каждый раз ясен).

Если каждый элемент множества A входит во множество B, то A называется *подмножеством* B, а B называется *надмножеством* A. Пишут $A\subseteq B$, $B\supseteq A$ (словами: A входит в B или A содержится в B, B содержит A). Очевидно, что если $A\subseteq B$ и $B\subseteq A$, то $A=B$. Пустое множество по определению считается подмножеством любого множества.

Если каждый элемент множества A входит в B, но множество B содержит хотя бы один элемент, не входящий в A, т. е. если $A\subseteq B$ и $A\neq B$, то A называется *собственным подмножеством* B, а B — *собственным надмножеством* A. В этом случае пишут $A\subset B$, $B\supset A$. Например, запись $A\neq 0$ и $A\supset 0$ означает одно и то же, именно, что множество A не пусто.

Заметим ещё, что надо различать элемент a и множество $\{a\}$, содержащее a в качестве единственного элемента. Такое различие диктуется не только тем, что элемент и множество играют неодинаковую роль (отношение $a\in A$ не симметрично), но и необходимостью избежать противоречия. Так, пусть $A=\{a, b\}$ содержит два элемента. Рассмотрим множество $\{A\}$, содержащее своим единственным элементом множество A. Тогда A содержит два элемента, в то время как $\{A\}$ — лишь один элемент, и потому отождествление этих двух множеств невозможно. Поэтому мы не будем применять запись $a\subset A$, сохраняя обозначение $a\in A$.

Примеры множеств. Примеров множеств можно привести сколько угодно. Так, можно говорить о множестве всех букв данной книги, причём одна и та же буква на разных страницах или разных строках одной страницы считается за два различных элемента множества, о множестве всех людей земного шара, причём надо сделать предположение, что в рассматриваемый момент времени

никто не рождается и не умирает, о множестве молекул воды в данном стакане и т. д.

Всё это — конечные множества. Приведём некоторые примеры бесконечных множеств, кроме упоминавшихся выше множеств натуральных чисел, чётных натуральных чисел, рациональных чисел, действительных чисел и др.

Пусть a и b — два действительных числа, причём $a<b$. Множество всех действительных чисел x, для которых $a\leqslant x\leqslant b$, называется *отрезком* с концами a, b и обозначается через $[a, b]$. Множество (a, b) всех x, для которых $a<x<b$, называется *интервалом* с концами a, b. Далее *полуинтервалами* называются множества $[a, b)$ тех x, для которых $a\leqslant x<b$, и $(a, b]$ тех x, для которых $a<x\leqslant b$. Введём ещё два символа: $+\infty$ (плюс бесконечность), $-\infty$ (минус бесконечность). Они не являются числами и вводятся лишь для удобства записи. Тем не менее для более лёгкого обращения с ними условимся говорить, что $+\infty$ больше, а $-\infty$ меньше любого действительного числа. Тогда можно ввести обозначения, аналогичные приведённым выше, для бесконечных полуинтервалов и интервалов. Именно: $[a, +\infty)$ — множество чисел x, для которых $a\leqslant x$, $(-\infty, b]$ — множество чисел x, для которых $x\leqslant b$, $(a, +\infty)$ — множество чисел x, для которых $a<x$, $(-\infty, b)$ — множество чисел x, для которых $x<b$, $(-\infty, +\infty)$ — множество всех действительных чисел.

§ 2. Операции над множествами

Объединением множеств A и B называется множество элементов, принадлежащих по крайней мере одному из данных множеств (т. е. либо A, либо B, либо одновременно и A и B). Пишут $A\cup B$ и читают «объединение A и B».

Пересечением множеств A и B называется множество элементов, принадлежащих одновременно и A и B. Пишут $A\cap B$ и читают «пересечение A и B».

Разностью множеств A и B называется множество элементов, принадлежащих A и не принадлежащих B. Пишут $A\setminus B$ и читают «разность A и B» [1]).

Пример 1. Пусть A есть отрезок $[1, 3]$, B — отрезок $[2, 4]$; тогда объединением $A\cup B$ будет отрезок $[1, 4]$, пересечением $A\cap B$ — отрезок $[2, 3]$, разностью $A\setminus B$ — полуинтервал $[1, 2)$, $B\setminus A$ — полуинтервал $(3, 4]$.

Пример 2. Пусть A есть множество прямоугольников, B — множество всех ромбов на плоскости. Тогда $A\cap B$ есть множество всех квадратов, $A\setminus B$ — множество прямоугольников с неравными сторонами, $B\setminus A$ — множество всех ромбов с неравными углами.

[1]) Некоторые авторы применяют обозначения $A+B$, AB, $A-B$, но в алгебре это не удобно из-за смешения с алгебраическими операциями.

Операции объединения и пересечения множеств обладают многими свойствами сложения и умножения чисел, например переместительным, сочетательным и распределительным свойствами.

Понятия объединения и пересечения множеств дословно переносятся на случай более двух множеств и даже на случай любого конечного или бесконечного множества множеств.

Для удобства речи будем называть *системами* такие множества, элементами которых служат другие множества. Тогда *объединением множеств некоторой системы* называется множество, состоящее из элементов, принадлежащих по крайней мере одному множеству данной системы. *Пересечением множеств некоторой системы* называется множество, состоящее из элементов, входящих во все множества данной системы.

Применяются следующие обозначения. В случае конечной системы множеств $A_1, A_2, \ldots, A_n$ объединение S и пересечение D обозначаются:

$$S = A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i,$$

$$D = A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i.$$

В случае бесконечной последовательности множеств $A_1, A_2, \ldots, A_n, \ldots$, т. е. системы, множества которой занумерованы всеми натуральными числами, пишут:

$$S = A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots = \bigcup_{i=1}^{\infty} A_i,$$

$$D = A_1 \cap A_2 \cap \ldots \cap A_n \cap \ldots = \bigcap_{i=1}^{\infty} A_i.$$

Пример 3. Пусть A_n есть множество точек плоскости, лежащих в круге радиуса 2^n с центром в точке O, причём n принимает все целые значения от $-\infty$ до $+\infty$. Тогда объединение $\bigcup_{n=1}^{+\infty} A_n$ совпадает со множеством точек всей плоскости, а пересечение $\bigcap_{n=1}^{+\infty} A_{-n}$ содержит лишь одну точку O.

Наконец, в случае произвольной системы $\{A_m\}$ множеств A_m, индексы которых составляют некоторое множество M, пишут:

$$S = \bigcup_{m \in M} A_m, \quad D = \bigcap_{m \in M} A_m.$$

Пример 4. Пусть X — множество всех положительных чисел x и A_x — множество точек круга радиуса x с центром в точке O. Тогда снова объединение $\bigcup_{x \in X} A_x$ будет множеством всех точек плоскости, а пересечение $\bigcap_{x \in X} A_x$ содержит лишь одну точку O.

§ 3. Функция, отображение, мощность

Понятие функции играет в математике такую же существенную роль, как понятие множества. Что же такое функция? Часто говорят, что функция есть переменная величина, зависящая от другой переменной величины (аргумента). В применении к обычным функциям, изучаемым в школе, как $y = \sin x$, это определение вполне подходит и может применяться в преподавании. Наша задача, однако, состоит в более точном уяснении сущности этого понятия и получении современного его определения. Прежде всего, если взять функцию

$$y = \sin^2 x + \cos^2 x,$$

то её значение уже не зависит от значения x. Далее, под величинами принято понимать такие объекты, которые можно сравнивать между собой, т. е. такие, между которыми существуют отношения б о л ь ш е и м е н ь ш е. Между тем в математике рассматриваются также и функции, для которых эти отношения не установлены, как, например, в случае комплексных чисел или вообще элементов некоторого множества. Внимательное рассмотрение показывает, что в понятии функции существенно не столько её изменение с изменением аргумента, сколько сам закон соответствия, в силу которого по каждому значению аргумента однозначно определяется соответствующее ему значение функции. Так функцию

$$y = \sin^2 x + \cos^2 x$$

можно определить, просто сказав, что каждому действительному числу x она ставит в соответствие число 1. Соответствие есть закон, позволяющий для каждого элемента x некоторого множества X однозначно указать некоторый объект (соответствующий данному элементу). Эти слова лишь поясняют понятие соответствия, но не должны пониматься как его определение. Понятие соответствия, как и понятие множества, принимается за основное, не подлежащее определению. Тогда наиболее общее определение функции будет такое:

О п р е д е л е н и е 1. *Функцией, заданной* (или *определённой*) *на некотором множестве X, называется соответствие, в силу*

которого любой элемент x множества X определяет некоторый (соответствующий ему) объект $f(x)$.

Множество X называется *областью определения функции,* а множество Y — объектов, соответствующих всем элементам множества X, — *областью значений функции.*

Пример 1. Пусть $y=\sin x$. За область определения функции можно принять множество действительных чисел. Тогда областью значений функции будет отрезок $[-1, +1]$.

Пример 2. Пусть $y=\operatorname{tg} x$. За область определения функции можно принять множество действительных чисел, отличных от чисел вида $n\pi+\frac{\pi}{2}$, где n пробегает все целые значения (ибо для этих значений x функция не определена). Тогда областью значений функции будет множество всех действительных чисел.

Пример 3. Функция Дирихле:

$$f(x)=\begin{cases} 0 \text{ при } x \text{ рациональном,} \\ 1 \quad \text{» } x \text{ иррациональном.} \end{cases}$$

Область определения здесь — множество действительных чисел, область значений — множество $\{0, 1\}$ из двух элементов.

Замечательно, что гениальный русский математик Н. И. Лобачевский более ста лет назад дал определение функции, весьма близкое к приведённому. В противовес господствовавшему тогда взгляду на функцию как на аналитическое выражение (т. е. как на формулу) он подчёркивал значение идеи соответствия в определении понятия функции.

«Это общее понятие, — писал Лобачевский о понятии функции, — требует, чтобы функцией от x называть число, которое даётся для каждого x и вместе с x постепенно изменяется. Значение функции может быть дано или аналитическим выражением или условием, которое подаёт средство испытать все числа и выбирать одно из них, или, наконец, зависимость может существовать и оставаться неизвестной» [1]).

Весьма близким к понятию функции является понятие отображения.

Определение 2. *Пусть даны два множества X и Y. Такое соответствие, при котором каждому элементу $x\in X$ соответствует (единственный) элемент $y\in Y$, называется отображением множества X в множество Y; в частности, если каждый элемент $y\in Y$ соответствует по крайней мере одному элементу $x\in X$, то такое соответствие называется отображением X на Y.*

---

[1]) Н. И. Лобачевский, Об исчезании тригонометрических строк. Учёные записки Казанского университета, кн. II, 1834.

Если элементу x соответствует y, то y называется *образом элемента x*, а x — *прообразом элемента y*. Пишут: $x \to y$ или $y = f(x)$. Множество A всех элементов $x \in X$, имеющих один и тот же образ $y \in Y$, называется *полным прообразом элемента y*.

Пример 4. Пусть D — множество действительных чисел. Соответствие $x \to |x|$ будет отображением множества D в себя же и отображением D на множество неотрицательных чисел. Прообразом числа 0 будет один 0, число $y > 0$ имеет два прообраза: $+y$ и $-y$.

Пример 5. Поставим в соответствие каждой точке квадрата её проекцию на основание. Получим отображение квадрата на отрезок. Полным прообразом каждой точки основания будет множество всех точек квадрата, лежащих на перпендикуляре к основанию, восставленном в данной его точке.

Примеры 4 и 5 показывают, что при отображении множества X в Y, с одной стороны, некоторые элементы из Y могут вовсе не иметь прообразов, а, с другой стороны, могут быть элементы, имеющие несколько (даже бесконечно много) прообразов. Если нет ни того, ни другого, то отображение называется *взаимно однозначным*. Таким образом, мы приходим к следующему определению:

Определение 3. *Взаимно однозначным соответствием между множествами X и Y* (или *отображением X на Y*) *называется соответствие* (соответственно, *отображение*), *обладающее следующими тремя свойствами:* 1) *каждому элементу множества X соответствует один и только один элемент множества Y;* 2) *двум различным элементам множества X всегда соответствуют два различных элемента множества Y;* 3) *всякий элемент множества Y соответствует хотя бы одному элементу множества X.*

Заметим, что первые два свойства дают взаимно однозначные отображения X на некоторое подмножество Y. В этом случае говорят о *взаимно однозначном отображении X в Y*.

Если $y = f(x)$ есть взаимно однозначное отображение X на Y, то каждому $y \in Y$ можно поставить в соответствие тот единственный элемент $x \in X$, образом которого при отображении f является y. Это соответствие называется *обратным отображением* для отображения f и обозначается через f^{-1}. В качестве упражнения предлагается доказать, что f^{-1} есть также взаимно однозначное отображение Y на X и что обратным для отображения f^{-1} будет исходное отображение f.

Определение 4. *Два множества X и Y, между которыми можно установить взаимно однозначное соответствие, называются равномощными* (или *эквивалентными*), *что обозначается символом $X \sim Y$.*

О равномощных множествах говорят также, что они имеют одинаковую мощность. Условимся считать, что пустое множество равномощно только самому себе.

Замечание. Выше мы дали определение понятия равномощности, но не понятие мощности. Можно сказать, что мощность есть то общее, что имеется у всех равномощных между собой множеств. Впрочем, всюду достаточно понятие равномощности.

Соотношение равномощности обладает следующими тремя основными свойствами:

1) рефлексивность: $X \sim X$;

2) симметрия: если $X \sim Y$, то $Y \sim X$;

3) транзитивность: если $X \sim Y$ и $Y \sim Z$, то $X \sim Z$.

Для доказательства, например, первого из них достаточно каждому элементу $x \in X$ поставить в соответствие его же самого (тождественное отображение), что уже даёт взаимно однозначное отображение множества X на себя. Доказательство остальных двух свойств предоставляется читателю.

Мощность множества характеризует, так сказать, «количество» его элементов. Однако при этом может оказаться, что «часть равна целому», т. е. множество может иметь одинаковую мощность с его собственным подмножеством.

Пример 6. Функция $y = 10x$, где x — действительное число, устанавливает равномощность отрезка $[0, 1]$ и в 10 раз более длинного отрезка $[0, 10]$. Таким образом, в смысле мощности «количество» точек обоих отрезков одинаково.

Пример 7. Два любых отрезка $[a, b]$ и $[c, d]$, а также два любых интервала (a, b) и (c, d) равномощны.

Для доказательства достаточно рассмотреть функцию

$$y = c + \frac{d-c}{b-a}(x-a).$$

Во-первых, каждому действительному числу x однозначно соответствует y, причём легко видеть, что $a \to c$ и $b \to d$. Далее, пусть

$$x_1 \to y_1, \quad x_2 \to y_2, \quad \text{и} \quad x_1 < x_2.$$

Согласно определению отрезка и интервала (см. стр. 82) $a < b$ и $c < d$. Следовательно, $\frac{d-c}{b-a} > 0$. Поэтому $y_1 < y_2$. Итак, если $a \leqslant x \leqslant b$ (или $a < x < b$), то и $c \leqslant y \leqslant d$ (соответственно, $c < y < d$). Значит, точкам отрезка $[a, b]$ соответствуют точки отрезка $[c, d]$, причём различные точки переходят в различные же (и то же верно в случае интервалов). Наконец, обратное отображение

$$x = a + \frac{b-a}{d-c}(y-c)$$

обладает теми же свойствами, откуда следует, что для каждого y из $[c, d]$ найдётся один (и даже только один) прообраз x из $[a, b]$

(то же для интервалов). Этим доказано, что $[a, b] \sim [c, d]$ (соответственно, $(a, b) \sim (c, d)$).

Пример 8. Функция $y = \operatorname{tg} x$ устанавливает эквивалентность интервала

$$\left(-\frac{\pi}{2}, +\frac{\pi}{2}\right)$$

множеству всех действительных чисел.

Пример 9. Считая соответствующими друг другу числа, стоящие одно под другим в следующих строках:

$$\begin{array}{llll} 1, & 2, & 3, \ldots, & n, \ldots, \\ 2, & 4, & 6, \ldots, & 2n, \ldots, \\ 1, & 3, & 5, \ldots, & 2n-1, \ldots, \\ 10, & 100, & 1000, \ldots, & 10^n, \ldots, \\ 2, & 3, & 5, \ldots, & p_n, \ldots \end{array}$$

(p_n — n-е — простое число),

мы заключаем, что множества всех натуральных чисел, чётных чисел, нечётных чисел, степеней 10, простых чисел все имеют одну и ту же мощность, хотя первая из них является собственным надмножеством остальных.

Пример 10. Множество натуральных чисел равномощно множеству рациональных чисел. В самом деле, любое рациональное число, отличное от нуля, однозначно записывается в виде несократимой дроби $\frac{p}{q}$, где принято $q > 0$ (т. е. знак отнесён к числителю).

Из возможных записей для нуля: $0 = \frac{0}{1} = \frac{0}{2} = \ldots$ выберем одну: $\frac{0}{1}$. Тогда запись вида $\frac{p}{q}$ однозначно определена для всех рациональных чисел (в частности, при $q = 1$ получатся все целые числа).

Высотой числа $\frac{p}{q}$ назовём натуральное число $|p| + q$, где $|p|$ — — абсолютная величина p. Тогда все рациональные числа можно расположить в одну последовательность, располагая их в порядке возрастания высоты, а числа с одинаковой высотой — в порядке возрастания числителя. Таким образом, получим последовательность

$$0, -1, +1, -2, -\frac{1}{2}, +\frac{1}{2}, +2, -3, -\frac{1}{3}, +\frac{1}{3} + 3,$$
$$-4, -\frac{3}{2}, -\frac{2}{3}, -\frac{1}{4}, +\frac{1}{4}, +\frac{2}{3}, +\frac{3}{2}, +4, \ldots$$

Так как чисел данной высоты n — лишь конечное число [именно, не более $2(n-1)$, ибо числитель меняется от $-(n-1)$ до $+(n-1)$, исключая значение 0], то перед каждым данным числом в последовательности стоит лишь конечное число чисел. Поэтому, нумеруя числа последовательно по порядку натуральными числами, мы действительно занумеруем все рациональные числа, что и доказывает требуемую равномощность.

§ 4. Конечные и бесконечные множества

Все указанные в предыдущем параграфе множества, равномощные собственным подмножествам, были бесконечны. Мы сейчас увидим, что это не случайно (см. ниже теорему 1). Однако сначала необходимо дать строгое определение понятия конечного и бесконечного множества. При этом нам придётся существенно использовать свойство натуральных чисел, строгое обоснование которых будет дано лишь в главе III. Читателю нужно убедиться, что в наших рассуждениях нет порочного круга. Для этого достаточно проверить, что при обосновании в главе III свойств натуральных чисел, применяемых в первых двух главах, мы нигде не пользуемся полученными в этих главах результатами.

Определение 1. *Множество натуральных чисел, меньших или равных некоторому натуральному числу n, называется отрезком натурального ряда и обозначается через* $|1, n|$.

Определение 2. *Множество, равномощное отрезку натурального ряда, а также пустое множество, называется конечным. Множество, не являющееся конечным, называется бесконечным.*

Иными словами, конечное множество (если оно не пусто) есть такое множество, элементы которого можно «пересчитать», т. е. перенумеровать так: $a_1, a_2, \ldots, a_n$, причём все элементы будут занумерованы, все числа от 1 до n будут использованы и различные элементы получат различные номера. Бесконечное же множество такое, элементы которого так «пересчитать» нельзя.

Из свойств 2) и 3) равномощности, приведённых в предыдущем параграфе, следует, очевидно, что множество, равномощное конечному (или бесконечному) множеству, само будет конечным (соответственно, бесконечным).

Теорема 1. (Основная теорема о конечных множествах.) *Конечное множество не равномощно никакому его собственному подмножеству и собственному надмножеству.*

Доказательство. Каждое из двух утверждений теоремы (о неравномощности подмножеству и надмножеству) легко следует из другого, так как, если $A \sim B$ и $A \supset B$, то из конечности одного из множеств A и B, как было отмечено выше, следует конечность другого. Докажем, например, что конечное множество A не равномощно его собственному подмножеству. Для пустого множества $A = 0$ теорема верна, так как пустое множество вовсе не имеет собственных подмножеств. Пусть $A \neq 0$. Тогда по определению конечного множества множество A равномощно (по крайней мере одному) отрезку натурального ряда $|1, n|$. Докажем индукцией по числу n[1]), что A нельзя взаимно однозначно отобразить на его соб-

[1]) Заметим, что нельзя вести индукцию по числу элементов множества A, так как понятие о числе элементов вводится ниже с применением теоремы 1.

ственное подмножество B. Для $n=1$ это очевидно, так как $A \sim |1, 1|$ и содержит лишь один элемент. Единственным его собственным подмножеством будет $B=0$, причём A не равномощно B.

Предположим, что теорема доказана для натурального числа n, и докажем её для числа $n+1$. Итак, пусть $A \sim |1, n+1|$, и f есть взаимно однозначное отображение A на B. Занумеровав элементы A соответствующими им числами, получим:

$$A=\{a_1, a_2, \ldots, a_{n+1}\}.$$

Для $B=0$ утверждение справедливо. Если $B \neq 0$, то без ограничения общности можно предположить, что $a_{n+1} \in B$. Иначе берём элемент $b \in B$ и строим новое множество B_1, полученное из B заменой элемента b на a_{n+1}, и новое отображение f_1, которое совпадает с f для всех элементов множества A, кроме элементов a со свойством $f(a)=b$, причём для этого элемента a полагаем $f_1(a)=a_{n+1}$. Тогда f_1 будет взаимно однозначным отображением A на собственное подмножество B_1, содержащее a_{n+1}. Далее, без ограничения общности можно считать, что $f(a_{n+1})=a_{n+1}$. Иначе пусть $f(a_i)=a_{n+1}$ и $f(a_{n+1})=a_j$. Тогда строим новое отображение f_1, совпадающее с f для всех элементов A, кроме a_i и a_{n+1}, причём полагаем $f_1(a_i)=a_j$ и $f_1(a_{n+1})=a_{n+1}$. Итак, пусть $a_{n+1} \in B$ и $f(a_{n+1})=a_{n+1}$, пусть также $A'=A \setminus \{a_{n+1}\}$ и $B'=B \setminus \{a_{n+1}\}$. Так как B — собственное подмножество A, то существует элемент $a' \in A \setminus B$. Так как $a_{n+1} \in B$, то $a' \neq a_{n+1}$. Поэтому $a' \in A \setminus B'$. Значит, B' есть собственное подмножество A'. Так как $f(a_{n+1})=a_{n+1}$, то отображение f устанавливает равномощность множеств A' и B', но $A'=\{a_1, a_2, \ldots, a_n\} \sim |1, n|$. Мы получили противоречие с предположением индукции, чем наше утверждение, а значит, и вся теорема доказаны.

Из теоремы 1 легко следует

Теорема 2. *Всякое непустое конечное множество равномощно одному и только одному отрезку натурального ряда.*

Доказательство. По определению 2 непустое конечное множество A равномощно по крайней мере одному отрезку натурального ряда. Если бы оно было равномощно двум различным отрезкам $A \sim |1, m|$, $A \sim |1, n|$, $m \neq n$, то по свойствам равномощности будет: $|1, m| \sim |1, n|$, что противоречит теореме 1, так как один из двух различных отрезков натурального ряда является собственным подмножеством другого.

Определение 3. *Однозначно определённое для данного непустого конечного множества A натуральное число n такое, что $A \sim |1, n|$, называется числом элементов множества A. Числом элементов пустого множества называется число* 0.

Из свойств равномощности следует, что два конечных множества тогда и только тогда равномощны, когда они имеют одно и то же

число элементов. Поэтому число элементов можно принять за определение мощности конечного множества.

Теорема 3. *Любое подмножество конечного множества само конечно. Любое надмножество бесконечного множества само бесконечно.*

Доказательство. Каждое из двух утверждений теоремы следует из другого. Так, если первое утверждение верно, то верно и второе, так как если A бесконечно и $A \subseteq B$, то и B бесконечно, ибо если бы B было конечно, то по первой половине теоремы и A было бы конечно. Достаточно поэтому доказать первое утверждение. Итак, пусть A конечно и $B \subseteq A$. Если $A = 0$, то и $B = 0$, теорема справедлива. Пусть $A \supset 0$. Тогда $A \sim |1, n|$ для некоторого натурального числа n. Применим индукцию относительно n. При $n = 1$ теорема верна, так как A содержит один элемент, и либо $B = 0$, либо $B = A$. Пусть утверждение верно для некоторого n. Докажем его для числа $n+1$. Итак, пусть f — взаимно однозначное отображение A на отрезок $|1, n+1|$. Если $B = A$, то B конечно. Пусть $B \subset A$. Существует элемент $a \in A \setminus B$. Можно считать, что $f(a) = n+1$. Иначе $f(a') = n+1$, где $a' \in A$, $a' \neq a$. Если тогда $f(a) = i$, то строим новое отображение f_1, полагая $f_1(a) = n+1$, $f_1(a') = i$ и $f_1 = f$ для остальных элементов множества A. Итак, пусть $f(a) = n+1$. Положим $A' = A \setminus \{a\}$. Тогда f определяет взаимно однозначное отображение множества A' на отрезок $|1, n|$, и $B \subseteq A'$. Следовательно, по предположению индукции B конечно. Теорема доказана.

Согласно теореме 3 понятие о числе элементов имеет смысл для любого подмножества данного конечного множества. При этом имеет место

Теорема 4. *Число элементов конечного множества A всегда больше числа элементов его собственного подмножества B.*

Доказательство. Пусть m — число элементов A и n — число элементов B. Предположим, что $n \geqslant m$. Так как $A \supset B$, то $A \neq 0$, $n > 0$ и $A \sim |1, m|$. Также и $n \geqslant m > 0$, следовательно,

$$B \sim |1, n|. \tag{1}$$

При взаимно однозначном отображении A на отрезок $|1, m|$ множество B отображается также взаимно однозначно на некоторое собственное подмножество B' отрезка $|1, m|$, таким образом,

$$B \sim B'. \tag{2}$$

Из $B' \subset |1, m|$ и $m \leqslant n$ следует:

$$B' \subset |1, n|. \tag{3}$$

Но из (1) и (2) вытекает $B' \sim |1, n|$, что в силу (3) противоречит теореме 1, ибо отрезок $|1, n|$ оказывается равномощным своему собственному подмножеству B'.

До сих пор мы ещё не доказали бесконечности какого-либо множества. Но из теоремы 1 следует

Теорема 5. *Множество N всех натуральных чисел, а также любое множество, содержащее подмножество, равномощное N, бесконечны.*

Доказательство. Множество N бесконечно, ибо отображение $f(n)=n+1$ для любого натурального числа n отображает взаимно однозначно $N=\{1, 2, 3, \ldots\}$ на его собственное подмножество $N_1=\{2, 3, 4, \ldots\}$. Значит, любое множество N', равномощное N, бесконечно, а по теореме 3 и любое множество, содержащее подмножество N', равномощное N, также бесконечно.

Примеры. Множества действительных или комплексных чисел содержат множество N натуральных чисел и, следовательно, бесконечны. Отрезок [0, 1] также есть бесконечное множество, так как он содержит множество N' чисел вида $\frac{1}{n}$ $(n=1, 2, 3, \ldots)$, равномощное N.

Определение 4. *Множество, равномощное множеству натуральных чисел, называется счётным.*

Иными словами, счётное множество — это такое множество, элементы которого можно «перенумеровать» при помощи натуральных чисел так, чтобы при этом все числа были использованы и различные элементы всегда имели бы различные номера. Таким образом, счётное множество A всегда можно записать в виде

$$A=\{a_1, a_2, \ldots, a_n, \ldots\}.$$

Как показывают примеры в конце предыдущего параграфа, множества чётных или нечётных чисел, а также множество рациональных чисел счётны.

Определение 5. *Множество, не являющееся конечным или счётным, называется несчётным.*

Следующий пример показывает, что такие множества действительно существуют [1]).

Множество всех действительных чисел несчётно. Заметим сначала, что из примеров 2 и 3 предыдущего параграфа следует равномощность этого множества интервалу (0, 1). Достаточно поэтому доказать несчётность последнего.

Мы будем считать известным, что каждое число интервала (0, 1) записывается в виде конечной или бесконечной десятичной дроби вида

$$0, a_1 a_2 a_3 \ldots$$

---

[1]) Существует даже бесконечно много различных мощностей, на чём мы останавливаться не будем, отсылая желающих к уже упомянутым выше книгам [1], стр. 40 или [2].

При этом хотя бы одна из цифр a_i отлична от нуля (ибо число $0 = 0{,}000\ldots$ не принадлежит интервалу). Далее, для чисел, имеющих запись в виде конечной десятичной дроби, существует и другая запись, где все цифры a_i, начиная с некоторого места, равны 9. Например,

$$0{,}53000\ldots = 0{,}52999\ldots$$

Остальные числа (т. е. иррациональные и те рациональные, которые разлагаются в периодическую дробь с периодом, не равным 9) имеют единственную запись [1]). Из двух возможных записей для первых чисел мы выберем какую-нибудь одну, например, в виде конечной десятичной дроби. Тогда все числа интервала (0, 1) будут единственным образом записываться в виде

$$0,\ a_1\ a_2\ a_3\ \ldots,$$

где не все a_i равны 0 и никогда все цифры, начиная с некоторой, не могут равняться 9. Обратно, всякая такая десятичная дробь даёт число интервала (0, 1).

Легко видеть, что интервал (0, 1) есть бесконечное множество, ибо он содержит множество

$$N' = \left\{ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \ldots \right\},$$

равномощное множеству натуральных чисел (см. теорему 5). Покажем, что (0, 1) не является счётным множеством.

Предположим обратное. Тогда все числа интервала можно занумеровать так:

$$(0,\ 1) = \{ c_1,\ c_2,\ c_3,\ \ldots \}.$$

Запишем каждое число десятичной дробью указанного вида:

$$\left.\begin{array}{l} c_1 = 0,\ a_{11}\ a_{12}\ a_{13},\ \ldots \\ c_2 = 0,\ a_{21}\ a_{22}\ a_{23}\ \ldots, \\ c_3 = 0,\ a_{31}\ a_{32}\ a_{33}\ \ldots, \\ \ldots\ldots\ldots\ldots \\ c_n = 0,\ a_{n1}\ a_{n2}\ a_{n3}\ \ldots, \\ \ldots\ldots\ldots\ldots \end{array}\right\} \qquad (4)$$

Построим теперь число

$$c = 0,\ b_1\ b_2\ b_3\ \ldots$$

следующим образом: берём цифру b_1, отличную от a_{11}, 0 и 9; берём b_2, отличную от a_{22}, 0 и 9; b_3, отличную от a_{33}, 0 и 9; b_n, отличную от a_{nn}, 0 и 9, ... Наличие десяти цифр оставляет для такого

[1]) См. стр. 253, А. Я. Хинчин, Элементы теории чисел.

выбора достаточно возможности (именно, каждый раз в нашем распоряжении остаётся ещё семь цифр). Дробь $0, b_1 b_2 b_3 \ldots$ обладает нужными свойствами и даже в усиленной форме — она вовсе не имеет цифр 0 и 9. Значит, число c принадлежит интервалу $(0, 1)$. Но запись c отлична от записей всех чисел (4). В самом деле, запись c отличается от c_1, ибо $b_1 \neq a_{11}$, от c_2, ибо $b_2 \neq a_{22}$ и т. д. Но дробью нашего типа числа интервала записываются однозначно. Значит,

$$c \neq c_1, \quad c \neq c_2, \quad c \neq c_3, \ \ldots, \ c \neq c_n, \ \ldots$$

Оказалось, что число c не входит во множество чисел (4), тогда как мы предположили, что в (4) перенумерованы все числа интервала. Полученное противоречие доказывает наше утверждение.

Среди всех бесконечных множеств счётные множества являются наименьшими в следующем смысле:

Теорема 6. *Всякое бесконечное множество содержит счётное подмножество.*

Доказательство. Пусть M — бесконечное множество. Тогда $M \neq 0$. Выберем какой-нибудь из его элементов и обозначим его через a_1. Пусть в M уже выбраны n различных между собою элементов $a_1, a_2, \ldots, a_n$. Так как M бесконечно, то

$$M \setminus \{a_1, a_2, \ldots, a_n\} \neq 0$$

и можно выбрать элемент

$$a_{n+1} \in M \setminus \{a_1, a_2, \ldots, a_n\}.$$

Он отличен от всех ранее выбранных элементов. По принципу индукции доказано, что для любого n существует в M подмножество $A_n = \{a_1, a_2, \ldots, a_n\}$ из n элементов, причём множество A_{n+1} получается из A_n присоединением одного нового элемента a_{n+1}. Очевидно, что объединение

$$A = \bigcup_{n=1}^{\infty} A_n = \{a_1, a_2, \ldots, a_n, \ldots\}$$

является счётным подмножеством M.

Теперь легко доказать, что свойство конечного множества не иметь равномощного ему собственного подмножества (см. теорему 1) для бесконечных множеств никогда не выполняется. Именно имеет место

Теорема 7. *Всякое бесконечное множество M равномощно некоторому собственному подмножеству.*

Доказательство. По теореме 6 множество M содержит счётное подмножество

$$A = \{a_1, a_2, \ldots, a_n, \ldots\}.$$

Пусть $M \setminus A = B$, $B \supseteq 0$. Определим отображение f множества M в себя следующим образом:

$$f(a_n) = a_{n+1} \ (n = 1, 2, \ldots), \ f(b) = b$$

для любого $b \in B$. Очевидно, что f является взаимно однозначным отображением множества M на его собственное подмножество $M \setminus \{a_1\}$, что и доказывает теорему.

Дадим теперь другое определение понятий конечного и бесконечного множеств.

Определение 2'. *Множество, не имеющее равномощного с ним собственного подмножества, а также пустое множество, называется конечным. Множество, не являющееся конечным, называется бесконечным.*

Из теорем 1 и 7 следует эквивалентность определения 2' прежнему определению 2. В самом деле, если множество конечно в смысле определения 2, то по теореме 1 оно конечно и в смысле определения 2'. Обратно, если множество конечно в смысле определения 2', то оно должно быть конечно и в смысле определения 2, так как иначе оно было бы бесконечно в смысле определения 2 и по теореме 7 бесконечно также в смысле определения 2', что невозможно. Итак, оба определения конечных множеств эквивалентны. Отсюда (посредством рассуждения от противного) сразу вытекает эквивалентность определений бесконечных множеств.

Отметим, что определение 2' имеет то (правда, лишь формальное) преимущество перед определением 2, что оно формулировано в терминах общей теории множеств, тогда как определение 2 предполагает известными свойства натурального ряда.

§ 5. Упорядоченные множества

До сих пор мы изучали лишь такие свойства множеств, которые были связаны с основным отношением, существующим между множеством и его элементами. Мы не рассматривали никаких соотношений между элементами одного и того же множества; все они были для нас совершенно равноправны. Однако в математике такие, так сказать, «чистые» множества встречаются редко. Обычно изучаются множества, между элементами которых существуют те или иные отношения, та или иная зависимость. Так, в геометрии две прямые в одной плоскости могут пересекаться или быть параллельными. Между тремя точками прямой существует отношение, выражаемое словами «одна из трёх точек лежит между двумя другими». В арифметике между числами существуют отношения $a + b = c$ или $ab = c$ и др. Одним из важнейших отношений, существующих между числами, является отношение порядка. Числа той или иной совокупности естественным образом располагаются в определённом

порядке, именно, в возрастающем порядке. Так, для множества натуральных чисел таким естественным порядком будет расположение

$$1,\ 2,\ 3,\ \ldots$$

В настоящем параграфе рассматривается понятие порядка в самом общем виде, т. е. для любых множеств.

Определение 1. *Множество M называется упорядоченным, если между его элементами установлено некоторое отношение $a<b$*[1]) *(читают: «a предшествует b»), обладающее следующими свойствами:* 1) *между любыми двумя элементами a и b существует одно и только одно из трёх соотношений: $a=b$, $a<b$, $b<a$;* 2) *для любых трёх элементов a, b и c из $a<b$, $b<c$ следует $a<c$.*

Пустое множество считается упорядоченным.

Замечание. Знак $=$ мы всегда понимаем в смысле тождества, совпадения элементов. Запись $a=b$ просто означает, что буквами a и b обозначен один и тот же элемент множества M. Поэтому из свойства 1) следует, что между двумя различными элементами выполняется одно и только одно из двух соотношений $a<b$ или $b<a$.

Если a предшествует b, то говорят, что b следует за a и пишут: $b>a$.

Отношение $a>b$ обладает, как легко проверить, свойствами, аналогичными 1) и 2). Его можно принять за основное, определив тогда через него отношение $a<b$ (см. ниже § 9).

Если в упорядоченном множестве M поменять ролями отношения $<$ и $>$, т. е. вместо $a<b$ писать $a>b$, и наоборот, то получится новое упорядоченное множество M', порядок которого называется *обратным* относительно порядка M. Например, для приведённого выше порядка во множестве натуральных чисел обратным будет порядок:

$$\ldots,\ 3,\ 2,\ 1.$$

Два упорядоченные множества, составленные из одних и тех же элементов, но расположенные в разном порядке, считаются различными. Поэтому при задании упорядоченного множества через его элементы необходимо указать их порядок. Мы будем считать, что запись слева направо соответствует порядку элементов, и сохраним прежнее обозначение фигурными скобками. Одно и то же множество можно упорядочить различным образом (если оно содержит не менее двух элементов). Так, множество натуральных чисел можно упорядочить обычным образом или в обратном порядке, можно нечётные числа поставить впереди чётных или наоборот, располагая те и дру-

[1]) Не следует смешивать смысла этой записи с неравенствами чисел.

гие в возрастающем или убывающем порядке. Получим упорядоченные множества

$$\{1, 2, 3, \ldots\}, \tag{1}$$

$$\{\ldots, 3, 2, 1\}, \tag{2}$$

$$\{1, 3, 5, \ldots, 2, 4, 6, \ldots\}, \tag{3}$$

$$\{1, 3, 5, \ldots, 6, 4, 2\}, \tag{4}$$

$$\{\ldots, 5, 3, 1, 2, 4, 6, \ldots\}, \tag{5}$$

$$\{\ldots, 5, 3, 1, \ldots, 6, 4, 2\}. \tag{6}$$

Элемент, не имеющий предшествующего, называется *первым*, а элемент, не имеющий следующего, — *последним*. Элементы a и b называются *соседними*, если не существует c, для которого $a<c<b$ или $b<c<a$. Если a и b — соседние и $a<b$, то говорят, что a непосредственно предшествует b, а b непосредственно следует за a. Упорядоченное множество (1) имеет первый элемент и не имеет последнего, множество (2), наоборот, имеет последний элемент, но не имеет первого, множество (4) имеет как первый элемент, так и последний, а множество (5) — ни первого элемента, ни последнего, множество (3) содержит два элемента, не имеющих непосредственно предшествующего, множество (6) — два элемента, не имеющих непосредственно следующего. Во всех этих множествах каждый элемент имеет соседний. Множество рациональных чисел, расположенных по возрастанию, не имеет соседних элементов, так как между любыми числами a и b лежит число $\frac{a+b}{2}$.

Если $a=b$ или $a<b$, то пишут: $a\leqslant b$; если $a=b$ или $a>b$, то пишут: $a\geqslant b$. Из определения 1 легко вытекает справедливость следующих двух теорем:

Теорема 1. *Если* $a\leqslant b$ *и* $b\leqslant a$, *то* $a=b$.

Теорема 2. *Если* $a\leqslant b$ *и* $b\leqslant c$, *то* $a\leqslant c$. *Если* $a\geqslant b$ *и* $b\geqslant c$, *то* $a\geqslant c$. *При этом, если хотя бы в одном из данных неравенств имеется строгое неравенство, то и в полученном неравенстве будет строгое неравенство.*

Определение 2. *Два упорядоченных множества* A *и* B *называются подобными, если между ними можно установить взаимно однозначное соответствие, сохраняющее порядок элементов, т. е. такое, что из*

$$a_1\to b_1,\quad a_2\to b_2 \text{ и } a_1<a_2$$

следует $b_1<b_2$.

Из определения 2 следует, что все множества, содержащие лишь один элемент, подобны и пустое множество подобно лишь самому себе. О подобных множествах говорят, что они имеют один и тот же тип. Отношение подобия обозначается так: $A\approx B$.

Читателю предоставляется доказать, что отношение подобия обладает следующими тремя свойствами:

I. Рефлексивность: $A \approx A$.

II. Симметрия: если $A \approx B$, то $B \approx A$.

III. Транзитивность: если $A \approx B$ и $B \approx C$, то $A \approx C$.

Сравнивая определение подобия с определением равномощности (§ 3, определение 4), мы убеждаемся, что первое включает второе, т. е. верна следующая

Теорема 3. *Подобные множества равномощны; из* $A \approx B$ *следует* $A \sim B$.

Обратное утверждение не верно. Так, множества (1) и (2) равномощны (даже просто равны как неупорядоченные множества), но не подобны, так как множество (1) имеет первый элемент, а множество (2) — не имеет, тогда как при соответствии подобия первому элементу одного множества должен соответствовать первый элемент другого. Тем не менее для конечных множеств теорема, обратная теореме 3, также верна. А именно:

Теорема 4. *Если конечные, упорядоченные множества равномощны, то они подобны.*

Эта теорема ввиду свойств I — III подобия является непосредственным следствием приведённой ниже теоремы 7. Для любых множеств в известной мере обратной теореме 3 является следующая теорема:

Теорема 5. *Любое множество A, равномощное упорядоченному множеству B, само можно упорядочить, т. е. определить для его элементов отношение порядка, обладающее свойствами* I *и* II [1]*, и притом так, что полученное упорядоченное множество подобно B.*

Доказательство. Если a_1 и a_2 — любые элементы множества A, b_1 и b_2 — соответствующие им, при взаимно однозначном отображении A на B, элементы B, и $b_1 < b_2$, то положим $a_1 < a_2$. Легко проверить, что определённое так отношение порядка в A обладает свойствами I и II и, очевидно, A подобно B.

Теорема 6. *Любое конечное упорядоченное множество A содержит первый и последний элемент* (если только A непусто).

Доказательство. Пусть A не имеет последнего элемента. Берём любой элемент $a_1 \in A$. Так как он не последний, то существует $a_2 \in A$ такой, что $a_1 < a_2$; так как a_2 — не последний, то существует $a_3 \in A$ такой, что $a_2 < a_3$. Если элемент a_n построен, то существует $a_{n+1} \in A$ такой, что $a_n < a_{n+1}$. По индукции элемент a_n построен для любого n. Пусть

$$N' = \{a_1, a_2, a_3, \ldots\}$$

---

[1]) Справедлива даже теорема, что любое множество можно, как говорят, вполне упорядочить (см. [1], стр. 99), но её доказательство выходит за рамки нашей статьи.

— множество всех построенных элементов. Очевидно, что из $i < k$ следует по свойству II $a_i < a_k$, откуда по свойству I $a_i \neq a_k$. Значит, N' равномощно множеству натуральных чисел. Поэтому множество A бесконечно (§ 4, теорема 5), что невозможно. Существование первого элемента доказывается аналогично.

Теорема 7. *Любое конечное множество можно упорядочить. Все конечные упорядоченные множества с одним и тем же числом элементов* $n > 0$ *подобны отрезку* $|1, n|$ *натурального ряда и, значит, подобны между собой.*

Доказательство. Пустое множество упорядочено по определению. Если $A \neq 0$ — конечное множество, то $A \sim |1, n|$. Отрезок $|1, n|$, очевидно, есть упорядоченное множество. По теореме 5 множество A можно упорядочить. Пусть теперь A — любое конечное упорядоченное множество с числом элементов $n > 0$. По теореме 6 множество A содержит первый элемент a_1. Если $n > 1$, то множество

$$A_1 = A \setminus \{a_1\} \neq 0$$

и снова содержит первый элемент a_2, причём $a_1 < a_2$. Пусть уже построен элемент a_i. Если $i < n$, то

$$A_i = A \setminus \{a_1, a_2, \ldots, a_i\} \neq 0$$

и по теореме 6 оно содержит первый элемент a_{i+1}, причём $a_i < a_{i+1}$. Так мы построим элементы a_i для всех $i \leqslant n$. Множество

$$A_n = \{a_1, a_2, \ldots, a_n\} \sim |1, n| \sim A.$$

Множество A не равномощно собственному подмножеству (§ 4, теорема 1). Значит,

$$A = A_n = \{a_1, a_2, \ldots, a_n\}.$$

Очевидно, что из $i < k$ следует $a_i < a_k$, т. е. A подобно отрезку $|1, n|$.

Из этой теоремы следует, что все $n!$ возможных перестановок множества с n элементами имеют один и тот же тип.

ГЛАВА II

ГРУППЫ, КОЛЬЦА И ПОЛЯ

§ 6. Группа

Арифметика и алгебра имеют дело с объектами различной природы: целыми, рациональными, действительными или комплексными числами, многочленами, алгебраическими дробями и т. д. При этом в первую очередь рассматриваются свойства основных четырёх действий: сложения, вычитания, умножения и деления.

Свойства этих действий для различных объектов во многом оказываются одними и теми же. Вот почему вполне естественным и весьма целесообразным является построение в современной алгебре самых общих образований, обладающих интересующими нас свойствами.

В таком абстрактном виде легче выяснить значение и взаимозависимость данных свойств, так как в конкретной области чисел, многочленов и т. д. дело осложняется наличием ряда других свойств помимо тех, которые мы желаем изучать.

В последующих главах будут изучаться основные числовые области. Чтобы лучше уяснить значение различных их свойств и одновременно избежать многократного повторения одних и тех же рассуждений в применении к каждой из этих областей, мы рассмотрим в настоящей главе основные понятия абстрактной алгебры. Читателю, желающему глубже изучить эти вопросы, рекомендуем статью Л. Я. Окунева [1]) и книги Л. Я. Окунева [3] и Б. Л. Ван-дер Вардена [4]. С точки зрения теории множеств любое из четырёх основных действий есть некоторое отношение между тройками элементов данного множества (см. начало § 5). Эти отношения отличаются, однако, от других (как, скажем, от отношения порядка, рассмотренного в § 5) тем, что во всех четырёх случаях по двум элементам находится третий (результат данного действия), дающий с двумя данными тройку элементов, находящихся в данном отношении. Отношения такого типа получили особое название, а именно:

---

[1]) Э. э. м., кп. 2., Л. Я. Окунев, Кольцо многочленов и поле рациональных функций.

Определение 1. *Соответствие, в силу которого каждой паре a, b элементов множества M, взятых в данном порядке, соответствует единственный третий элемент с того же множества M, называется алгебраической операцией, определённой в M.*

Используя понятие функции (§ 3, определение 1), можно сказать короче, что алгебраическая операция, определённая во множестве M, есть функция, определённая на множестве всех упорядоченных пар элементов M, значения которой принадлежат M.

Примерами алгебраических операций могут служить четыре арифметических действия: сложение $a+b=c$, вычитание $a-b=c$, умножение $a\cdot b=c$, деление $a:b=c$, рассматриваемые хотя бы на множестве всех действительных чисел, причём в случае деления нужно исключить число 0, деление на которое не определено. Дальнейшими примерами являются сложение, вычитание, умножение и деление комплексных чисел, сложение векторов по правилу параллелограмма, сложение, вычитание и умножение многочленов и т. д.

Как известно, две или более алгебраических операций могут быть связаны между собою переменой роли данных и искомых элементов. Так, если $a+b=c$, то $c-a=b$; если $ab=c$, то $a=\frac{c}{b}$. Эта связь операций выражает понятие обратной операции, которое в общем виде определяется так:

Пусть дана операция, ставящая в соответствие паре элементов a, b из M элемент c. Те две операции, которые получатся из данной путём перемены в ней роли одного из элементов a, b и элемента c (одного из данных элементов с искомым), называются *обратными* для данной операции.

Таким образом, первая обратная операция паре c, b ставит в соответствие a, а вторая — паре c, a ставит в соответствие b. Как хорошо известно, обратные операции не всегда существуют или не всегда единственны. Так, для натуральных чисел определены операции сложения и умножения, но обратные операции — вычитание и деление — не всегда выполнимы.

Операция называется *коммутативной*, если её применение к парам a, b и b, a всегда даёт один и тот же результат. Ниже мы увидим, что если для коммутативной операции существует одна из обратных операций, то существует и другая и обе они совпадают. Для некоммутативной операции это уже неверно.

Так, для положительных действительных чисел операция $f(a, b)=a^b$ не коммутативна, ибо $a^b\neq b^a$. Первая обратная операция $f_1(c, b)=\sqrt[b]{c}$ существует; вторая же — $f_2(c, a)=\log_a c$ не определена для $a=1$ и $c\neq 1$, а также для таких a и c, когда $\log_a c\leqslant 0$ (ведь мы рассматриваем нашу операцию лишь на множестве положительных чисел). В тех же случаях, когда вторая операция также определена, она не совпадает с первой операцией.

В одном и том же множестве может быть задано несколько алгебраических операций. Желая изучать общие свойства сложения и умножения чисел, мы рассмотрим сначала множества с одной алгебраической операцией. Таким образом, мы приходим к первому из основных понятий современной алгебры, именно к понятию группы.

Определение 2. *Непустое множество G называется группой, если в нём определена алгебраическая операция, называемая умножением, которая каждым двум элементам a, b из G ставит в соответствие элемент ab также из G, называемый их произведением, и обладает нижеследующими свойствами*:

I. (Закон ассоциативности.) $a(bc)=(ab)c$ [1]);

II. (Закон обратимости.) *Для любых a и b из G уравнения $ax=b$ и $ya=b$ разрешимы в G, т. е. в G существуют элементы c и d такие, что $ac=b$, $da=b$.* Если групповая операция коммутативна, т. е. $ab=ba$ для любых a, b из G, то группа G называется *коммутативной* [2]).

Приведём несколько примеров групп.

Пример 1. Все целые, все рациональные, все действительные и все комплексные числа являются группами относительно операции сложения чисел, играющего роль групповой операции умножения.

Ни одно из этих множеств не является группой относительно операции умножения чисел, ибо уравнения $0 \cdot x = 1$ не имеют решения.

Пример 2. Все рациональные, все действительные и все комплексные числа, исключая число 0, являются группами относительно операции умножения чисел.

Пример 3. Множество G двух элементов e и a с операцией, заданной равенствами $ee=aa=e$, $ea=ae=a$, является группой.

Все эти группы коммутативны.

Пример 4. Пусть G — множество всех взаимно однозначных отображений множества M на себя (§ 3, определение 3). Образ элемента $a \in M$ при отображении $s \in G$ будем обозначать через as. Произведением st двух отображений s и t из G назовём отображение, полученное в результате последовательного выполнения данных отображений (сначала s, затем t), т. е. полагаем

$$a(st)=(as)t$$

для любого $a \in M$ [3]). При таком определении операции умножения множество G является группой. В самом деле, закон ассоциативности I

---

[1]) Знак $=$ обозначает, как всегда, совпадение элементов.

[2]) Коммутативные группы называются также абелевыми.

[3]) Можно под произведением st понимать выполнение сначала t, а затем s. Тогда образ элемента a при отображении s удобнее обозначить через sa.

выполнен, так как если r, s, t — три любых элемента из G, то для любого a из M находим:

$$a[r(st)] = (ar)(st) = [(ar)s]t.$$

Но также

$$a[(rs)t] = [a(rs)]t = [(ar)s]t.$$

Таким образом,

$$a[r(st)] = a[(rs)t]$$

для любого a из M. Это значит, что $r(st) = (rs)t$ (оба отображения получаются в результате последовательного выполнения данных отображений r, s, t).

Докажем выполнение в G закона обратимости II. Пусть s и t — любые отображения из G. Для взаимно однозначного отображения s существует также взаимно однозначное обратное отображение s^{-1} (§ 3). Именно, если $as = b$, то $bs^{-1} = a$. Очевидно, что $ss^{-1} = s^{-1}s = e$, где e — тождественное отображение множества M на себя, и что $ex = xe = x$ для любого отображения x из G. Предположим, что в G существует отображение u такое, что $su = t$. Умножая это равенство слева на s^{-1}, получим:

$$s^{-1}(su) = s^{-1}t.$$

По закону ассоциативности найдём: $s^{-1}(su) = (s^{-1}s)u = eu = u$, т. е. $u = s^{-1}t$. Итак, уравнение $sx = t$ может иметь решение лишь $s^{-1}t$. Но это отображение действительно удовлетворяет уравнению $sx = t$, так как

$$s(s^{-1}t) = (ss^{-1})t = et = t.$$

Аналогично доказывается, что уравнение $ys = t$ имеет единственное решение $y = ts^{-1}$.

Итак, G — группа. Она называется *группой преобразования множества* M. Для конечного M группа G называется также *группой подстановок множества* M.

Если M содержит более двух элементов, то группа подстановок G не коммутативна. Так, группа подстановок трёх чисел 1, 2, 3 содержит шесть элементов. Обозначая каждую подстановку двумя строками, где под каждым числом стоит число, ему соответствующее, запишем их в виде

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Перемножая, находим:

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \quad \text{и} \quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

т. е. произведение меняется при перемене порядка сомножителей.

Группы подстановок имеют большое значение в алгебре. С ними связано решение вопроса о разрешимости уравнения в радикалах, данное французским математиком Эваристом Галуа (1811—1832).

Следствия из законов ассоциативности и коммутативности. Закон ассоциативности I позволяет говорить о произведении трёх элементов a, b и c группы G, понимая под этим любое из равных произведений $a(bc)$ и $(ab)c$, и писать рядом abc без скобок. Можно, однако, и без закона ассоциативности индуктивно определить произведение

$$a_1 a_2 \dots a_n = \prod_{i=1}^{n} a_i$$

для любых n элементов $a_1, a_2, \dots, a_n$ из G (обоснование законности индуктивного определения будет дано в гл. III). Именно:

Определение 3. $\prod_{i=1}^{1} a_i = a_1$ *для любого элемента* a_1 *из* G; $\prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i\right) a_{n+1}$.

Согласно этому определению имеем, например:

$$a_1 a_2 a_3 = (a_1 a_2)\, a_3,$$

$$a_1 a_2 a_3 a_4 = [(a_1 a_2)\, a_3]\, a_4,$$

$$a_1 a_2 a_3 a_4 a_5 = \{[(a_1 a_2)\, a_3]\, a_4\}\, a_5 \text{ и т. д.}$$

Произведение двух произведений также можно представить в виде произведения всех встречающихся элементов, а именно:

$$(a_1 a_2 \dots a_m)(a_{m+1} a_{m+2} \dots a_n) = a_1 a_2 \dots a_n$$

или в сокращённой записи:

$$\prod_{i=1}^{m} a_i \prod_{k=1}^{n-m} a_{m+k} = \prod_{i=1}^{n} a_i. \qquad (1)$$

Докажем равенство (1) при заданном m индукцией по n. При $n = 1$ оно вытекает прямо из определения 3. Если (1) верно для

числа n, то, применяя определение 3 и закон ассоциативности, находим:

$$\prod_{i=1}^{m} a_i \prod_{k=1}^{n+1} a_{m+k} = \prod_{i=1}^{m} a_i \left(\prod_{k=1}^{n} a_{m+k} \cdot a_{m+n+1} \right) =$$

$$= \left(\prod_{i=1}^{m} a_i \prod_{k=1}^{n} a_{m+k} \right) a_{m+n+1} =$$

$$= \prod_{i=1}^{m+n} a_i \cdot a_{m+n+1} = \prod_{i=1}^{m+n+1} a_i,$$

что и доказывает (1) для числа $n+1$.

Можно определить произведение любого конечного числа элементов группы с любым распределением скобок и доказать его независимость от распределения скобок [5].

Для коммутативной группы G произведение n элементов не зависит от порядка сомножителей, т. е. если $f(i)$ — любое взаимно однозначное отображение множества 1, 2, ... , n на себя, то

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{f(i)}. \qquad (2)$$

Наметим лишь ход доказательства, предоставляя читателю его детальное проведение. 1) Пользуясь правом вводить и отбрасывать скобки и законом коммутативности, доказываем, что произведение n элементов не меняется от перестановки двух соседних множителей. 2) Перестановку двух любых множителей сводим к ряду перестановок соседних множителей. 3) Любую перестановку множителей сводим к ряду перестановок двух множителей.

Следствия из законов обратимости. Заметим, что свойство II ещё не означает наличия в G операций, обратных умножению, так как II утверждает лишь существование, но не единственность элементов c и d. Для доказательства единственности этих элементов введём понятия единицы и обратного элемента.

Определение 4. *Единицей группы G называется элемент e такой, что $ea = ae = a$ для любого a из G. Обратным для элемента a из G называется элемент a^{-1} такой, что $aa^{-1} = a^{-1}a = e$, где e — единица группы G.*

Теорема 1. *В любой группе G существует единица e и притом только одна; для любого элемента a существует обратный элемент a^{-1} и притом только один; существующие по закону обратимости* II *решения уравнений $ax = b$ и $ya = b$ являются единственными для любых a и b из G.*

Доказательство. Пусть e — решение уравнения $yb=b$ для некоторого b из G, т. е. $eb=b$. Для любого a уравнение $bx=a$ имеет решение c, т. е. $bc=a$. Тогда

$$ea=e(bc)=(eb)c=bc=a.$$

Итак, $ea=a$ для любого a из G. Так же доказывается существование в G элемента e' такого, что $ae'=a$ для любого a из G.

Тогда $e=ee'=e'$. Итак, e — единица группы G. Если e_1 и e_2 — две единицы, то $e_1=e_1e_2=e_2$, чем доказана единственность единицы e.

Далее, по закону обратимости II существуют элементы b и c, для которых $ba=e$ и $ac=e$. Тогда $b=be=b(ac)=(ba)c=ec=c$, т. е. $b=c$.

Итак, элемент $a^{-1}=b$ обладает свойством $aa^{-1}=a^{-1}a=e$, т. е. является обратным для a. Если b и c — два любых элемента, обратных для a, то, как выше, докажем, что $b=bac=c$, чем доказана единственность обратного элемента.

Если c_1 и c_2 — любые решения уравнения $ax=b$, то $ac_1=b$ и $ac_2=b$. Значит, $ac_1=ac_2$. Умножая слева на a^{-1}, найдём $c_1=c_2$. Так же доказывается единственность решения уравнения $ya=b$. Теорема доказана.

Заметим, что из существования во множестве G единицы и обратных элементов при наличии закона ассоциативности следует выполнение в G законов обратимости. В самом деле, уравнение $ax=b$ имеет решение $a^{-1}b$ и уравнение $ya=b$ имеет решение ba^{-1}. Таким образом, группу можно было бы определить как множество с ассоциативной операцией, обладающее единицей и обратными элементами.

В примере 1 групп чисел по сложению единицей будет число 0 и обратным элементом для числа a — противоположное число — a. В примере 2 групп чисел по умножению единицей будет число 1 и обратным элементом для числа a — обратное число $\frac{1}{a}$. В примере 3 единицей будет e и каждый из элементов e и a будет обратным для самого себя. В примере 4 единицей будет тождественное отображение множества M на себя, и обратным элементом для отображения s будет обратное отображение s^{-1}.

Произведение n одинаковых сомножителей a называется n-й *степенью* a и обозначается через a^n.

Это определение имеет смысл для любого натурального числа n. Для $n=0$ определяем $a^0=e$, где e — единица группы G. Для целого отрицательного $n=-m$ степень $a^n=a^{-m}$ можно определить либо как $(a^{-1})^m$, либо как $(a^m)^{-1}$. Оба эти определения эквивалентны, так как

$$a^m(a^{-1})^m=\underbrace{(aaa\ \dots\ a)}_{m\text{ раз}}\underbrace{(a^{-1}a^{-1}a^{-1}\ \dots\ a^{-1})}_{m\text{ раз}}=e,$$

откуда $(a^{-1})^m=(a^m)^{-1}$.

Свойство произведения (1) при совпадении сомножителей обращается в известное свойство степени

$$a^m a^n = a^{m+n}. \tag{3}$$

Далее, индукцией по n легко доказать, что

$$(a^m)^n = a^{mn}. \tag{4}$$

Для коммутативных групп из возможности перестановки сомножителей (2) следует:

$$(ab)^n = a^n b^n. \tag{5}$$

Мы указали, как равенства (3), (4) и (5) доказываются для натуральных чисел m и n, однако эти равенства остаются верными для любых целых чисел m и n, что можно проверить путём рассмотрения всевозможных случаев $m \gtreqless 0$, $n \gtreqless 0$.

Из однозначности решений уравнений $ax = b$ и $ya = b$ следует наличие в группе G обеих обратных операций для операции умножения. В случае коммутативной группы G обе эти обратные операции совпадают. В самом деле, если c — решение уравнения $ax = b$, то $ac = b$. Значит, $ca = b$, т. е. c — решение уравнения $ya = b$.

Определение 5. *Операция, обратная для операции умножения в коммутативной группе G, называется делением. Её результат для элементов a и b, т. е. решение уравнений $ax = b$ и $ya = b$, называется частным элементов b и a и обозначается через $b : a$ или $\frac{b}{a}$.*

Аддитивная запись. Групповая операция может обозначаться через $a + b$ и называться *сложением*. Тогда говорят об аддитивной записи группы. В этом случае группа обычно предполагается коммутативной. При аддитивной записи вместо 1 говорят о нуле и вместо обратного элемента a^{-1} о противоположном элементе — a. Далее, вместо степени a^n говорят о кратном na (не следует понимать na как произведение n и a, ибо целое число может и не быть элементом группы G). Итак,

$$na = \underbrace{a + a + a + \ldots + a}_{n \text{ раз}}.$$

Для аддитивно записанной группы G сумма n элементов обозначается так:

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i,$$

и соответственно изменяется вид равенств (1) — (5). В частности, равенства (3) — (5) принимают вид

$$(m+n)\,a = ma + na, \tag{6}$$

$$m\,(na) = (mn)\,a, \tag{7}$$

$$n\,(a+b) = na + nb. \tag{8}$$

Операция, обратная операции сложения в аддитивно записанной коммутативной группе, называется *вычитанием*, а её результат для элементов a и b, т. е. решение уравнений $a+x=b$ и $y+a=b$, называется *разностью* элементов b и a и обозначается через $b-a$.

Подгруппа. Определение 6. *Подмножество H группы G называется подгруппой этой группы, если оно само является группой при той же групповой операции, что и в G.*

При выяснении того, является ли данное подмножество H подгруппой, можно пользоваться следующей теоремой:

Теорема 2. *Непустое подмножество H группы G будет подгруппой тогда и только тогда, когда* 1) *произведение двух любых элементов a и b из H принадлежит H,* 2) *элемент a^{-1}, обратный для любого элемента a из H, принадлежит к H.*

Доказательство. Необходимость этих условий очевидна. Если, обратно, для H выполнены условия 1) и 2), то H (как непустое множество) содержит элемент a, значит, по свойству 2) оно содержит и a^{-1} и по свойству 1) $a\,a^{-1}=e$. Таким образом, H содержит единицу e и вместе с любым элементом a содержит обратный элемент a^{-1}. Так как закон ассоциативности автоматически переходит с G на H, то H — подгруппа группы G.

Мы ограничимся лишь этими основными свойствами групп, отсылая читателя, интересующегося более глубокими свойствами, к специальной литературе (см. [6] и [7]).

§ 7. Кольцо

Мы рассмотрели в предыдущем параграфе свойства одной алгебраической операции. Однако в случае чисел, которыми мы будем заниматься в дальнейшем, налицо две операции — сложение и умножение, — связанные между собою дистрибутивным (распределительным) законом. В этом и следующем параграфах мы и рассмотрим общие свойства множеств с двумя операциями. При этом мы ограничимся лишь нужным для чисел случаем коммутативных операций.

Определение 1. *Непустое множество R называется кольцом, если в нём определены две алгебраические операции: сложение, ставящее в соответствие каждым двум элементам a, b элемент $a+b$, называемый их суммой, и умножение, ставящее в соответствие каждым двум элементам a, b элемент ab, называемый их*

произведением, причём эти операции обладают следующими свойствами:

I. (Коммутативность сложения.) $a+b=b+a$;

II. (Ассоциативность сложения.) $a+(b+c)=(a+b)+c$;

III. (Обратимость сложения.) *Для любых* a *и* b *из* R *уравнение* $a+x=b$ *имеет* (по крайней мере одно) *решение, т. е. существует элемент* $c\in R$ *такой, что* $a+c=b$;

IV. (Коммутативность умножения.)[1]) $ab=ba$;

V. (Ассоциативность умножения.) $a(bc)=(ab)c$;

VI. (Дистрибутивность умножения относительно сложения.)

$$(a+b)c=ac+bc.$$

Примеры колец. При обычных операциях сложения и умножения кольцом является:

1. Множество целых чисел.
2. Множество рациональных чисел.
3. Множество действительных чисел.
4. Множество комплексных чисел.
5. Множество, состоящее лишь из одного числа 0.
6. Множество чётных чисел и вообще множество целых чисел, кратных некоторому числу n.
7. Множество комплексных чисел $a+bi$ с целыми a и b (так называемое кольцо целых комплексных чисел).
8. Множество действительных чисел $a+b\sqrt{2}$, где a и b — целые числа.

Множество натуральных чисел, а также множество всех положительных рациональных чисел кольцами не являются, так как не выполняется аксиома III.

9. Большую роль в алгебре играет кольцо многочленов с одним или несколькими неизвестными и коэффициентами из некоторого кольца R.

При этом за операции сложения и умножения принимаются обычные действия над многочленами, известные из школьной алгебры. Эти действия имеют смысл, так как они сводятся к сложению и умножению коэффициентов многочленов, а последние принадлежат к кольцу R, где указанные действия определены.

10. Пары (a, b) целых чисел образуют кольцо, если операции определены по формулам

$$(a, b)+(c, d)=(a+c, b+d),\quad (a, b)(c, d)=(ac, bd).$$

---

[1]) В литературе термин «кольцо» применяется также ко множествам с некоммутативным или даже неассоциативным умножением. Формулировки других свойств также меняются. В конце данной статьи при обобщении понятия числа нам понадобятся кольца без коммутативности умножения.

Проверить справедливость аксиом I—VI во всех этих примерах предоставляется читателю.

Для сложения и умножения в кольце справедливы все следствия, полученные из законов ассоциативности и коммутативности в предыдущем параграфе. В частности, можно определить сумму и произведение любого конечного числа элементов (§ 6, определение 3), для которых верны правила оперирования, аналогичные (1) из § 6 и которые не зависят от порядка данных элементов [§ 6, (2)].

Свойства I—III показывают, что кольцо относительно операции сложения является коммутативной группой. Поэтому во всяком кольце существует элемент 0, называемый нулём кольца, со свойством

$$a+0=0+a=a$$

для любого a. Далее, для любого a существует противоположный элемент $-a$ такой, что

$$a+(-a)=(-a)+a=0.$$

При совпадении слагаемых или сомножителей мы получаем n-кратное na или n-ю степень a^n элемента a. При этом степень a^n определена вообще лишь для натурального n, так как её определение для $n\leqslant 0$ требовало существование единицы и обратного элемента a^{-1}, что в кольце может не выполняться. Свойства степени (3)—(5) из § 6 сохраняются также лишь для натуральных показателей. В отличие от этого понятие n-кратного na элемента a и его свойства (6)—(8) из § 6 остаются верными в случае кольца (как группы по сложению) для любых целых чисел.

Из законов сложения I—III следует (как для всякой коммутативной группы) существование в любом кольце операции вычитания, обратной сложению. Умножение может и не обладать обратной операцией, как, например, в кольце целых чисел или в кольце многочленов.

Следствие закона дистрибутивности. До сих пор мы рассматривали свойства каждой из двух операций кольца отдельно. Переходим к изучению их связи между собой. Эта связь определяется законом дистрибутивности VI.

Прежде всего из VI и IV следует, очевидно, вторая форма закона дистрибутивности:

$$a(b+c)=ab+ac.$$

Далее, обе формы закона дистрибутивности оказываются верными также и для разности, т. е.

$$(a-b)c=ac-bc,\quad a(b-c)=ab-ac. \tag{1}$$

Для доказательства первого равенства надо проверить, что элемент $(a-b)c$ удовлетворяет определению разности элементов ac и bc. Но действительно

$$bc+(a-b)c=[b+(a-b)]c=ac.$$

Второе равенство доказывается аналогично.

Докажем теперь, что нуль кольца обладает обычным свойством при умножении:

Теорема 1. *Если один из сомножителей равен нулю, то и всё произведение равно нулю, т. е.*

$$a\cdot 0=0,\quad 0\cdot a=0 \tag{2}$$

для любого a.

Докажем лишь первое из равенств, так как второе вытекает из первого при помощи IV. По определению нуля и разности $0=b-b$ для любого b. Отсюда $a\cdot 0=a(b-b)=ab-ab=0$.

Однако теорема, обратная теореме 1, верная для чисел, уже не сохраняется для любых колец, иными словами, если произведение двух элементов кольца равно нулю, то нельзя утверждать, что хотя бы один из них равен нулю. Так, в приведённом выше примере 10 кольца, составленного из пар (a, b) целых чисел, нулём является, очевидно, пара (0, 0). Если взять целые числа $a\neq 0$ и $b\neq 0$, то пары $(a, 0)$ и $(0, b)$ отличны от нуля кольца, но $(a, 0)(0, b)=(0, 0)$.

Определение 2. *Элементы a и b кольца, для которых $a\neq 0$, $b\neq 0$, но $ab=0$, называются делителями нуля. Кольцо без делителей нуля называется также областью целостности.*

Теорема 2. *Из $ab=ac$ следует $b=c$, если только $a\neq 0$ и не является делителем нуля.*

Доказательство. Из $ab=ac$ следует $ab-ac=0$ или $a(b-c)=0$. Но так как $a\neq 0$ и не делитель нуля, то $b-c=0$, $b=c$.

В дальнейшем нам придётся иметь дело исключительно с кольцами без делителей нуля. Для них из $ab=ac$ и $a\neq 0$ следует $b=c$.

При умножении справедливы обычные правила знаков [1]), а именно:

$$a(-b)=-ab,\quad (-a)b=-ab,\quad (-a)(-b)=ab. \tag{3}$$

Первое из этих равенств доказывается так:

$$ab+a(-b)=a[b+(-b)]=a\cdot 0=0,$$

откуда $a(-b)=-ab$.

---

[1]) Заметим, что не следует пользоваться терминами «положительный» и «отрицательный» элемент, как для чисел. Эти понятия для любых колец будут введены в § 10. Пока же элементы a и $-a$ вполне равноправны, каждый из них является противоположным для другого, и если обозначить $-a$ через b, то a придётся обозначить через $-b$.

Второе вытекает из первого:

$$(-a)\,b = b\,(-a) = -ba = -ab.$$

Третье следует из первых двух:

$$(-a)\,(-b) = -(-a)\,b = -(-ab) = ab.$$

По индукции законы дистрибутивности обобщаются на любое конечное число слагаемых, а затем и на произведение двух сумм. Справедливы, таким образом, равенства

$$\left.\begin{aligned} \Big(\sum_{i=1}^{n} a_i\Big)\,b = \sum_{i=1}^{n} a_i b, \quad a\sum_{i=1}^{n} b_i = \sum_{i=1}^{n} ab_i, \\ \Big(\sum_{i=1}^{n} a_i\Big)\Big(\sum_{k=1}^{m} b_k\Big) = \sum_{i=1}^{n}\Big(\sum_{k=1}^{m} a_i b_k\Big). \end{aligned}\right\} \tag{4}$$

Отсюда и из свойств кратного [§ 6, (7)] при совпадении слагаемых каждой суммы, т. е. при

$$a_i = a \ \ (i = 1,\ 2,\ \ldots,\ n),\quad b_k = b \ \ (k = 1,\ 2,\ \ldots,\ m),$$

следует далее:

$$\left.\begin{aligned} (na)\,b = a\,(nb) = n\,(ab), \\ (na)\,(mb) = n\,[m\,(ab)] = (nm)\,(ab). \end{aligned}\right\} \tag{5}$$

В главе IV нам понадобятся следующие свойства разности элементов кольца:

Теорема 3. (Свойства разности.) *В любом кольце разность элементов обладает следующими свойствами:*

а) $a - b = c - d$ *тогда и только тогда, когда* $a + d = b + c$;

б) $(a - b) + (c - d) = (a + c) - (b + d)$;

в) $(a - b) - (c - d) = (a + d) - (b + c)$;

г) $(a - b)(c - d) = (ac + bd) - (ad + bc)$.

Доказательство. Прибавляя $b + d$ к обеим частям равенства $a - b = c - d$, получим: $a + d = b + c$. Обратно, прибавляя $(-b) + (-d)$ к обеим частям второго из этих равенств, получим первое. Этим доказано а). Равенства б), в) и г) доказываются аналогично.

Подкольцо. Определение 3. *Подмножество M кольца R называется подкольцом, если оно само является кольцом при тех же операциях сложения и умножения, которые определены в кольце R.*

Так, кольцо чётных чисел является подкольцом кольца целых чисел, а последнее в свою очередь — подкольцом кольца рациональных чисел.

При выяснении того, является ли данное множество кольца подкольцом, нет надобности проверять справедливость всех свойств кольца. Большинство из них автоматически переходит с кольца на любое его подмножество. Удобнее всего пользоваться для этого такой теоремой:

Теорема 4. *Для того чтобы непустое подмножество M кольца R было его подкольцом, необходимо и достаточно, чтобы сумма, разность и произведение любых двух элементов из M снова принадлежали M.*

Доказательство. Для доказательства необходимости этих условий предположим, что M является подкольцом R. Сложение в M совпадает со сложением в R. Но из единственности обратной операции следует, что и вычитание в M совпадает с вычитанием в R. Поэтому сумма, разность и произведение любых двух элементов из M (определённые в кольце R) должны принадлежать снова к M, так как иначе одна из этих операций для данных двух элементов M была бы невыполнима в M, что противоречит определению кольца (см. определение 1) и следующей из него выполнимости вычитания.

Для доказательства достаточности предположим, что множество M удовлетворяет условиям теоремы. Так как сумма и произведение (определённые в R) любых элементов из M снова принадлежат к M, то их можно принять за результат сложения и умножения в M. Этим в M будут определены сложение и умножение. Свойства I, II, IV, V и VI переносятся автоматически с R на любое его подмножество и, значит, выполнены в M. Пусть a и b — элементы M. Тогда $b-a=c$ также есть элемент M. Но по свойству разности в R имеем:

$$a+(b-a)=b \quad \text{или} \quad a+c=b.$$

Таким образом, и свойство III выполнено в M, и M является подкольцом кольца R.

§ 8. Поле

Примеры колец, приведённые в предыдущем параграфе, показывают, что в отношении обратной операции для умножения (в отличие от сложения) различные кольца обладают совершенно различными свойствами. Так, в кольце целых чисел деление выполняется лишь в исключительных случаях, причём все элементы кольца делятся на $+1$ и -1. В кольце же рациональных чисел деление всегда возможно (кроме деления на 0). Желая изучить свойства обратной операции для умножения, мы приходим к важнейшему частному случаю кольца — полю.

Определение 1. *Полем называется кольцо P, обладающее следующими свойствами:*

VII. (Обратимость умножения.) *Для любых a и b из P, где $a \neq 0$, уравнение $ax = b$ имеет* (по крайней мере одно) *решение, т. е. существует элемент $q \in P$ такой, что $aq = b$.*

VIII. *P содержит по крайней мере один элемент, отличный от нуля.*

Примеры полей. Из примеров 1—10 колец, приведённых в предыдущем параграфе, только 2, 3 и 4, т. е. рациональные, действительные и комплексные числа, являются полями. В примере 5 свойство VII выполнено, так как вообще нет элемента $a \neq 0$, но не выполнено свойство VIII. В остальных примерах не выполняется свойство VII. Приведём ещё следующие примеры полей.

1. Множество комплексных чисел $a + bi$ с любыми рациональными a, b (так называемое поле рациональных комплексных чисел; сравнить с примером 7 из § 7).

2. Множество действительных чисел вида $a + b\sqrt{2}$ с любыми рациональными a и b (сравнить с примером 8 из § 7).

3. Множество всех рациональных функций с действительными коэффициентами от одного или нескольких переменных.

4. Множество из двух элементов, которые мы обозначим через 0 и 1, при следующем определении операций:

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1,$$
$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Проверку свойств I — VIII мы предоставляем читателю.

Все теоремы из § 7, выведенные для колец, остаются верными, в частности, для полей. Кроме того, из свойства VII вытекают теоремы, аналогичные тем, которые были выведены в § 7 из свойства III.

Как всякое кольцо, поле является группой относительно операции сложения. Все элементы поля, не равные нулю, образуют группу относительно операции умножения. В самом деле, если $a \neq 0$ и $b \neq 0$, то уравнение $ax = b$ имеет решение $q \neq 0$, ибо $a \cdot 0 = 0 \neq b$ (§ 7, теорема 1). Поэтому свойства умножения IV, V (§ 7, определение 1) и VII доказывают наше утверждение. Группа по сложению всех элементов поля называется *аддитивной*, а группа по умножению всех его элементов, отличных от нуля, — *мультипликативной группой поля*. Поле вполне определяется заданием двух этих групп, заданием произведений нуля на все элементы и требованием дистрибутивного закона для любых его элементов, включая нуль. Отсюда уже следует, что произведение любого элемента на нуль равно нулю (§ 7, теорема 1).

Из свойств мультипликативной группы (§ 6, теорема 1) следует, что в поле существует единица, т. е. такой элемент e, что $ae = ea = a$ для любого a из P. В самом деле, для $a \neq 0$ это следует из свойств единицы группы, а для $a = 0$ — из свойства нуля при умножении.

Далее, для любого $a \neq 0$ существует обратный элемент a^{-1} такой, что $aa^{-1} = a^{-1}a = e$. При этом единица e и обратный элемент a^{-1} для данного a определяются однозначно.

Если в кольце существует единица, то только одна, ибо, если e_1 и e_2 — единицы, то $e_1 = e_1 e_2 = e_2$. Если для элемента a кольца с единицей существует обратный элемент, то только один, ибо, если b и c — обратные элементы для a, то $b = bac = c$.

Но в кольце с единицей может и не быть обратных элементов, как, например, в кольце целых чисел. Существуют также кольца без единицы, как, например, кольцо чётных чисел или кольцо целых чисел, кратных числу $n > 1$.

Если в кольце R существует единица $e \neq 0$ и для любого $a \neq 0$ существует обратный элемент a^{-1}, то элементы кольца, отличные от нуля, образуют группу по умножению (§ 6), и значит, кольцо R будет полем.

Так как мультипликативная группа поля коммутативна, то умножение обладает обратной операцией — делением. При этом частное $\frac{b}{a}$ однозначно определено для любого a, не равного нулю, и любого b. Для $b \neq 0$ это следует из свойств мультипликативной группы поля (§ 6), а для $b = 0$ имеем: $\frac{0}{a} = 0$, так как $a \cdot 0 = 0$. Дополнительное требование $a \neq 0$, входящее в свойство VII, нарушает симметрию свойств сложения и умножения поля. Отбросить это требование и тем самым восстановить указанную симметрию, однако, невозможно. В самом деле, уравнение $ax = b$ при $a = 0$ и $b \neq 0$ не имеет решения в поле или даже в кольце, содержащем элементы, отличные от нуля. Действительно, если q — решение указанного уравнения, то $aq = 0 \cdot q = 0 = b$, что невозможно. Поэтому деление на нуль невозможно, если делимое отлично от нуля. Частное $\frac{0}{0}$ может равняться любому элементу кольца, так как для любого q имеем: $0 \cdot q = 0$.

Теорема 1. *Поле не имеет делителя нуля* (§ 7, определение 2), *т. е. если* $ab = 0$, *то либо* $a = 0$, *либо* $b = 0$.

Доказательство. Если $ab = 0$ и $a \neq 0$, то, умножая обе части равенства на a^{-1}, найдём $1 \cdot b = a^{-1} \cdot 0$, т. е. $b = 0$.

Итак, поле является кольцом без делителей нуля. Утверждение, обратное этому, вообще неверно: существуют кольца без делителей нуля (например, кольцо целых чисел), не являющиеся полями. Однако для конечных колец обратная теорема также верна. А именно:

Теорема 2. *Всякое конечное кольцо без делителей нуля, содержащее более одного элемента, является полем.*

Доказательство. Достаточно проверить свойство VII. Пусть $a \neq 0$. Каждому элементу x кольца поставим в соответствие элемент $y = ax$. Если $x_1 \neq x_2$, то также $y_1 \neq y_2$, ибо иначе $ax_1 = ax_2$ и $x_1 = x_2$ (§ 7, теорема 2). Значит, $x \to y$ есть взаимно однозначное

отображение всего кольца R на некоторое его подмножество M, т. е. $R \sim M$. Но по теореме 1 из § 4 конечное множество R не равномощно своему собственному подмножеству. Поэтому $R = M$, т. е. для любого элемента $b \in R$ существует в R элемент q такой, что $q \to b$, т. е. $aq = b$, что и доказывает VII.

Так как все элементы поля, отличные от нуля, образуют по умножению коммутативную группу, то для любого элемента $a \neq 0$ степень a^n определена при любом целом показателе n, причём справедливы обычные свойства степени [см. § 6, (3)—(5)].

Для частного элементов любого поля верны те же правила оперирования, что и для обыкновенных дробей. В главе V нам понадобятся следующие свойства частного:

Теорема 3. (Свойства частного.) а) *Если* $b \neq 0$, $d \neq 0$, *то* $\frac{a}{b} = \frac{c}{d}$ *тогда и только тогда, когда* $ad = bc$;

б) *если* $b \neq 0$, $d \neq 0$, *то* $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$;

в) *если* $b \neq 0$, $d \neq 0$, *то* $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

г) *если* $b \neq 0$, $c \neq 0$, $d \neq 0$, *то* $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$.

Доказательство. Помножая обе части равенства $\frac{a}{b} = \frac{c}{d}$ на bd, получим: $ad = bc$. Если, обратно, дано равенство $ad = bc$, где $b \neq 0$ и $d \neq 0$, то, полагая $\frac{a}{b} = x$, $\frac{c}{d} = y$, получим: $bdx = ad$, $bdy = bc$, откуда $bdx = bdy$. Умножая обе части равенства на b^{-1} и d^{-1}, получим: $x = y$, т. е. $\frac{a}{b} = \frac{c}{d}$.

Этим утверждение а) доказано. Утверждения б) и в) доказываются аналогично второй части утверждения а). Наконец, для доказательства утверждения г) достаточно убедиться, что

$$\frac{a}{b} = \frac{c}{d} \cdot \frac{ad}{bc}.$$

Но это равенство следует, очевидно, из в) и а). Теорема доказана.

Характеристика поля. Существуют поля, содержащие элементы $a \neq 0$ такие, что $na = 0$ при целом n, отличном от нуля. Так, в поле из двух элементов 0 и e (см. пример 4 в начале этого параграфа) имеем: $2e = e + e = 0$. Справедливо утверждение:

Теорема 4. *Для любого поля* P *имеет место один из двух случаев*:

а) *для любого элемента* $a \neq 0$ *и любого целого числа* $n \neq 0$ *кратное* na *также отлично от нуля*;

б) *существует единственное простое число*[1]) p *такое, что* $pa=0$ *для любого элемента* a.

Доказательство. Пусть случай а) не имеет места, т. е. существуют элемент поля $a\neq 0$ и целое число $n\neq 0$, для которых $na=0$. Докажем, что тогда имеет место случай б). Для любого $b\in P$ существует q такое, что $aq=b$. Тогда по (5) из § 7 также

$$nb=n(aq)=(na)q=0\cdot q=0.$$

Достаточно поэтому доказать, что случай б) имеет место для какого-нибудь одного элемента $a\neq 0$, например для единицы e. По доказанному $ne=0$, значит, и $(-n)e=-ne=0$. Одно из чисел n и $-n$ — положительное. Существуют, следовательно, натуральные числа k такие, что $ke=0$. Пусть p будет наименьшее из чисел k с этим свойством[2]).

Покажем, что p — число простое; $p\neq 1$, так как $1\cdot e=e\neq 0$ и $pe=0$. Если p делится на q, где $1<q<p$, то $p=qr$ и также $1<r<p$. Тогда по (5) из § 7

$$pe=(qr)(ee)=(qe)(re)=0,$$

и ввиду отсутствия делителей нуля (теорема 1) либо $qe=0$, либо $re=0$, что невозможно, ибо p — наименьшее натуральное число, обладающее этим свойством. Пусть k — любое натуральное число такое, что $ke=0$; деля k на p, найдём: $k=pq+r$, где остаток r удовлетворяет условию $0\leqslant r<p$. Тогда из (6) § 6 и (5) § 7 следует:

$$ke=(pq+r)e=(pq)e+re=q(pe)+re=0+re=re=0.$$

Значит, должно быть $r=0$, так как $r>0$ противоречит выбору p. Итак, $k=pq$, т. е. k делится на p, и если k отлично от p, оно не может быть простым. Значит, p — единственное простое число, для которого $pe=0$.

Эта теорема позволяет дать следующее определение:

Определение 2. *Характеристикой поля* P *называется число* 0, *если* $na\neq 0$ *для любого элемента* $a\neq 0$ *и любого целого числа* $n\neq 0$ *и простое число* p *такое, что* $pa=0$ *для любого элемента* a *в противном случае.*

Так как для числа 1 и любого целого n будет $n\cdot 1=n$, то все числовые поля имеют характеристику 0.

Пример поля характеристики $p>0$. Пусть n — любое натуральное число, большее единицы. Тогда все целые числа могут быть разбиты на классы, так что к одному классу принадлежат все

---

[1]) Под простым числом понимается натуральное число, отличное от 1 и не делящееся ни на какое натуральное число, кроме 1 и самого себя.

[2]) Что всякое непустое множество натуральных чисел содержит наименьшее число, будет доказано в главе III.

числа, дающие при делении на n один и тот же остаток. Если класс чисел, дающих при делении на n остаток r, обозначить через (r), то мы получим всего n различных классов: (0), (1), (2), ..., $(n-1)$. Очевидно, что два числа a и b тогда и только тогда принадлежат к одному классу, когда их разность $a-b$ делится на n[1]). Пусть C_n — множество всех определённых таким образом классов целых чисел. Определим в C_n операции сложения и умножения. Если (r) и (s) — два класса, причём класс (r) содержит число a и (s) — число b, то суммой $(r)+(s)$ данных классов назовём класс, содержащий число $a+b$, и произведением $(r)\cdot(s)$ — класс, содержащий число ab. Сумма и произведение классов определены однозначно, т. е. не зависят от выбора представителей a и b этих классов. В самом деле, если a и a' — два числа из класса (r) и b и b' — два числа из класса (s), то числа $a-a'$ и $b-b'$ делятся на n. Поэтому также

$$(a+b)-(a'+b')=(a-a')+(b-b')$$

и

$$ab-a'b'=(ab-a'b)+(a'b-a'b')=(a-a')\,b+a'\,(b-b')$$

делятся на n. Но это значит, что числа $a+b$ и $a'+b'$ принадлежат к одному классу и то же верно для чисел ab и $a'b'$.

Свойства кольца I—VI (§ 7, определение 1) для классов автоматически выполняются, так как эти свойства верны для целых чисел, и операции над классами определены через операции над представителями. Итак, C_n является кольцом. Оно называется *кольцом вычетов по модулю n*. Нулём кольца C_n является, очевидно, класс (0), состоящий из всех чисел, делящихся на n.

Если $n=kl$ — число составное, то кольцо C_n содержит делитель нуля, так как $(k)\neq(0)$ и $(l)\neq(0)$, но $(k)\cdot(l)=(0)$. Если же $n=p$ — число простое, то кольцо C_p не имеет делителей нуля, так как, если $(r)\cdot(s)=(0)$, то rs делится на p, и значит, либо r, либо s делится на p, т. е. либо $(r)=0$, либо $(s)=0$.

Так как кольцо C_p содержит p элементов и, значит, конечно, то по теореме 2 оно будет полем. Класс $p(r)$ содержит число pr, делящееся на p. Поэтому $p\cdot(r)=(0)$ для любого класса (r) поля C_p.

Значит, p — характеристика поля C_p.

Подполе. Простое поле. Определение 3. *Множество M поля P называется подполем P, если оно само является полем при тех же операциях сложения и умножения, которые заданы в поле P. Тогда P называется надполем или расширением поля M.*

Так, поле рациональных чисел является подполем поля действительных чисел, а последнее — подполем поля комплексных чисел.

---

[1]) По существу мы имеем здесь дело со сравнениями по модулю n (см. статью А. Я. Хинчина в этой книге).

Теорема 5. *Для того чтобы множество M поля P, содержащее не менее двух элементов, было подполем, необходимо и достаточно, чтобы сумма, разность, произведение и частное* (если только оно существует в P) *любых элементов из M снова принадлежали к M.*

Доказательство вполне аналогично проведённому для соответствующей теоремы о кольцах (см. § 7, теорема 4), и мы его приводить не будем.

Всякое подполе M поля P содержит 0 как разность $a-a$, где $a \in M$, и единицу как частное $\frac{a}{a}$, где $a \in M$, $a \neq 0$.

Теорема 6[1]). *Пересечение* (в смысле пересечения множеств; см. § 2) *любого множества подполей поля P опять является подполем поля P.*

Доказательство. Пусть $\{M_s\}$ есть некоторое множество подполей, где индексы s образуют множество S и $D \bigcap\limits_{s \in S} M_s$ — пересечение всех подполей M_s данного множества; 0 и 1 входят в каждое подполе M_s и, значит, в D. Итак, D содержит не менее двух элементов. Если a и b — элементы D, то они входят в каждое M_s и по теореме 5 $a+b$, $a-b$, ab, а при $b \neq 0$ и $\frac{a}{b}$ также входят в M_s, а значит, и в D. В силу теоремы 5 D — подполе поля P.

Определение 4. *Поле, не имеющее подполей, отличных от него самого, называется простым.*

Примерами простых полей могут служить поле рациональных чисел и поля вычетов по простому модулю p.

Любое подполе M поля P рациональных чисел содержит число 1, а значит, и все его кратные $n \cdot 1 = n$, т. е. все целые числа, а значит, и все их частные, т. е. все рациональные числа. Итак, $M = P$, т. е. P — простое поле. Точно так же любое подполе M поля C_p вычетов по простому модулю p содержит класс (1), служащий единицей C_p, а значит, любой класс (r) как r-кратное класса (1). Итак, $M = C_p$, т. е. C_p — простое поле.

Можно доказать, что этими полями в некотором смысле исчерпываются все простые поля.

Теорема 7. *Любое поле содержит простое подполе и притом только одно.*

Доказательство. Поле P вообще содержит подполя (например, само P). Пусть D есть пересечение всех подполей поля P. По теореме 6 D является подполем P и по самому определению входит в любое подполе. Пусть M — подполе D, отличное от D.

---

[1]) Соответствующая теорема верна и для колец, т. е. пересечение любого множества подколец кольца R есть подкольцо кольца R. Доказательство её вполне аналогично данному здесь для полей и предоставляется читателю.

Из определения 3 следует, очевидно, что M будет подполем и для P, и D не входит в M, что невозможно. Итак, D — простое подполе P. Если D' — также простое подполе поля P, то пересечение $D''=D\cap D'$ будет опять подполем поля P, причём $D''\subseteq D$ и $D''\subseteq D'$. Но из определения 3 следует, что в таком случае D'' будет подполем как для D, так и для D', а так как D и D' — простые подполя, то $D=D''=D'$, чем доказана единственность простого подполя.

§ 9. Аксиоматическое построение математики. Изоморфизм

Каждая математическая теория изучает множества с теми или иными отношениями элементов, обладающими теми или иными свойствами. Содержание теории заключается в определении одних отношений (или понятий) через другие и в доказательстве одних свойств этих отношений (или понятий) на основании других свойств. Так, в теории упорядоченных множеств одно из отношений «больше» и «меньше» определяется через другое, с их помощью определяется понятие «первый элемент» и т. д. (§ 5); в теории колец отношение $a-b=c$ и понятие «нуль» определяются через отношение $a+b=c$.

Ясно, что определить все понятия и отношения и доказать все их свойства невозможно по причинам чисто логического характера: каждое определение лишь сводит данное понятие к другим, а каждое доказательство лишь выводит данное свойство из других. Приходится поэтому некоторые отношения (или понятия) оставлять без определения. Они называются *основными отношениями* или понятиями. Точно так же приходится некоторые свойства этих основных отношений оставлять без доказательства. Эти свойства называются *основными свойствами* или *аксиомами*. Список основных понятий и аксиом и составляет фундамент данной математической теории, на котором вся она строится логическими средствами.

Основной особенностью, придающей современному построению математических наук абстрактный характер, является изучение свойств интересующих нас понятий и отношений в применении к любым множествам, в которых данные понятия и отношения могут быть определены. При этом конкретный смысл элементов множеств и все их конкретные свойства (помимо изучаемых в данной математической теории) для данной теории совершенно безразличны. Так именно было, например, в трёх последних параграфах при определении группы, кольца и поля как множеств элементов с данными отношениями (операциями сложения и умножения), обладающими данными основными свойствами; так обстоит дело при аксиоматическом построении геометрии (см. [8] и [9]), где точки, прямые и плоскости — объекты, природа которых для формального построения геометрии совершенно безразлична, лишь бы между ними были определены

основные отношения («точка лежит на прямой» и т. п.), удовлетворяющие основным условиям (аксиомам геометрии).

Но если так, то можно думать, что существует не одна, а много теорий колец и полей, не одна, а много различных геометрий в зависимости от того, какое конкретное множество положено в основу данной теории. Выход из этого затруднения следует, однако, уже из сказанного выше и заключается в точном определении содержания данной математической теории. Ведь данная теория, как было указано, изучает не все свойства элементов множества, а лишь те из них, которые относятся к основным отношениям, заданным для этих элементов, и которые вытекают из основных свойств (аксиом), которым подчиняются основные отношения. Все остальные свойства (сами по себе, может быть, весьма важные) просто не являются предметом изучения в данной теории. Она абстрагируется от этих свойств. Поэтому все множества, для элементов которых определены (для каждого множества по-своему, на основе конкретных свойств его элементов) основные отношения и у которых все свойства этих отношений одинаковы, с точки зрения данной теории неразличимы между собой.

Но так как основные отношения определяются для каждого множества, исходя из конкретных свойств его элементов, то, изучая в абстрактной форме свойства основных отношений, данная теория изучает, таким образом, некоторые конкретные свойства целого класса конкретных множеств. Это диалектическое единство абстрактного и конкретного свойственно всякой науке, но в математике оно проявляется, пожалуй наиболее ярко. Конечно, математика изучает не все свойства материальных тел, а лишь те из этих свойств, которые поддаются количественной оценке или пространственному описанию. Основные для всей математики понятия числа и фигуры являются абстрактным выражением именно этих свойств материальных тел. Таким образом, несмотря на абстрактный характер построения современной математики, для неё остаётся в силе определение, данное Энгельсом [1]):

«Чистая математика имеет своим объектом пространственные формы и количественные отношения действительного мира, стало быть — весьма реальный материал. Тот факт, что этот материал принимает чрезвычайно абстрактную форму, может лишь слабо затушевать его происхождение из внешнего мира».

Понятие множеств, имеющих одинаковые свойства отношений между их элементами и поэтому неразличимых в рамках данной математической теории, получает точное выражение в следующем общем понятии изоморфизма:

Определение 1. *Два множества M и M', в каждом из которых определены отношения элементов, образующие некоторую*

[1]) Ф. Энгельс, Анти-Дюринг, 1948, стр. 37.

систему отношений S, называются изоморфными (*запись $M \cong M'$*) *относительно данной системы отношений* (короче просто *изоморфными*), *если между ними существует взаимно однозначное соответствие, сохраняющее все отношения системы S, т. е. такое, что если любые элементы M находятся в любом из отношений системы S, то соответствующие им элементы M' находятся в том же отношении, и обратно.*

Можно сказать, что аксиоматическая теория изучает множества лишь с точностью до изоморфизма относительно системы основных отношений данной теории.

Понятие изоморфизма обладает, очевидно, тремя основными свойствами:

1) $M \cong M$,

2) если $M \cong M'$, то $M' \cong M$,

3) если $M \cong M'$ и $M' \cong M''$, то $M \cong M''$.

Например, в случае отсутствия каких-либо отношений (в случае, когда система отношений S есть пустое множество) определение 1 обращается в определение эквивалентности (§ 3), а в случае одного отношения «a предшествует b» при выполнении соответствующих аксиом — в отношение подобия (§ 5).

То, что понятие изоморфизма действительно выражает одинаковость всех рассматриваемых свойств множеств, можно формулировать в виде следующего общего положения:

Если множества M и M' изоморфны относительно некоторой системы отношений S, то любое свойство множества M, формулированное в терминах отношений системы S (и, значит, и отношений, определяемых через отношения системы S), *переносится на множество M', и обратно.*

Разберём это положение на конкретном примере.

Пусть в множествах M и M' определено отношение «больше», и они изоморфны относительно этого отношения; тогда, если M упорядочено, т. е. если в M выполнены свойства 1) и 2) из § 5, то они выполнены и в M'.

Докажем свойство 1). Пусть a' и b' — элементы M' и a и b — соответствующие элементы M. В силу условия 1) в M выполнено одно из соотношений $a = b$, $a > b$, $b > a$. Отображение M на M' сохраняет отношение «больше». Значит, выполнено одно из соотношений $a' = b'$, $a' > b'$, $b' > a'$. Если бы в M' выполнялось более одного из них, то из сохранения отношения «больше» при отображении M' на M следовало бы выполнение более одного отношения для a и b, что противоречит условию 1).

Докажем свойство 2). Если $a' > b'$ и $b' > c'$, то также $a > b$ и $b > c$. В самом деле, в M должно быть $a > c$. Значит, $a' > c'$.

Займёмся теперь изоморфизмом групп колец и полей. Ввиду того, что здесь отношения $a + b = c$ и $ab = c$ удовлетворяют дополнительным требованиям, что для любых a и b существует одно и

только одно c, для которого $a+b=c$ или $ab=c$ (эти два требования являются по существу двумя дополнительными аксиомами), причём эти требования предполагаются выполненными как в M, так и в M', определение изоморфизма групп колец и полей можно упростить по сравнению с определением 1, а именно требовать сохранения основных отношений лишь при переходе от M к M'. Ограничиваясь случаем колец и полей, нужным в дальнейшем при определении числовых областей (случай групп отличается от рассмотренного лишь тем, что налицо одна операция вместо двух), получаем таким образом:

Определение 2. *Кольцо* (или поле) R *называется изоморфным кольцу* (соответственно *полю*) R' (запись $R\cong R'$), *если существует взаимно однозначное отображение* R *на* R', *при котором сумме и произведению любых элементов* R *соответствуют сумма и произведение соответствующих элементов* R'.

Покажем, что это определение является частным случаем общего определения 1. Для этого надо лишь убедиться, что обратное отображение R' на R также сохраняет сумму и произведение. Пусть в R' имеем: $a'+b'=c'$, и элементам a', b', c' при обратном отображении соответствуют a, b, c из R. Надо доказать, что $a+b=c$. Но если $a+b=d\neq c$, то из определения 2 следовало бы $a'+b'=d'\neq c'$, что противоречит однозначности операции сложения в R'.

В последнем рассуждении мы не пользовались аксиомами кольца I—VI. Поэтому определение 2 дословно переносится на любые множества, в каждом из которых задано две алгебраические операции — сложение и умножение.

Теорема 1. *Пусть* R *и* R' *— множества, в каждом из которых определены операции сложения и умножения. Пусть* R *изоморфно* R' (в смысле определения 2). *Тогда, если* R *есть кольцо* (или *поле*), *то и* R' *будет кольцом* (соответственно *полем*).

Доказательство. Достаточно убедиться в справедливости для R' аксиом I—VI или I—VIII (§ 7, определение 1 и § 8, определение 1). Во всех случаях (кроме аксиомы VIII, где доказательство очевидно) рассуждение совершенно одинаково. Докажем, например, аксиому III. Пусть a' и b' — элементы R' и a и b — их прообразы в R. Так как в R аксиома III выполнена, то существует элемент $c\in R$ такой, что $a+c=b$. Если $c\to c'$, то в силу изоморфизма также $a'+c'=b'$, т. е. c' есть решение уравнения $a'+x'=b'$. Значит, R' также обладает свойством III. Читателю рекомендуется доказать справедливость в R' остальных аксиом.

Вместе с основными свойствами при изоморфизме сохраняются и все другие свойства, являющиеся следствиями основных. Так, при изоморфизме колец R и R' нулю R соответствует нуль R', и если R содержит единицу, то и R' содержит единицу, причём она соответствует единице из R. В самом деле, из $a+0=a$ в R следует

$a'+0'=a'$ в R' и из $a\cdot 1=a$ в R следует $a'\ 1'=a'$ в R' для любого элемента a' из R'.

Большое значение при построении числовых полей будет иметь следующая, почти очевидная:

Теорема 2. *Пусть R — подкольцо кольца S и R' — кольцо, изоморфное R и не имеющее общих элементов с S. Тогда для любого данного изоморфного отображения f кольца R на R' существует кольцо S', содержащее в качестве подкольца R' и изоморфное кольцу S, причём существует изоморфное отображение g кольца S на S', созпадающее на R с данным отображением f, т. е. такое, что $g(a)=f(a)$ для любого элемента a из R. Если S — поле, то и S' будет полем. Если R — подполе S, то и R' — подполе S'.*

Доказательство. Пусть S' — множество, полученное из S путём замены элементов R на элементы R', т. е. $S'=(S\setminus R)\cup R'$. Строим такое отображение g множества S на S': если $a\in S\setminus R$, то положим $g(a)=a$; если $a\in R$, то положим $g(a)=f(a)$, где $f(a)$ — элемент R', соответствующий a при данном изоморфизме f.

Так как f — взаимно однозначное отображение R на R', g — взаимно однозначное отображение $S\setminus R$ на себя и множества S и R' не имеют общих элементов (достаточно даже, чтобы $S\setminus R$ и R' не имели общих элементов), то g является взаимно однозначным отображением S на S'.

Операции сложения и умножения в S' определим через операции в S путём перенесения их в S' с помощью отображения g, т. е. положим

$$g(a)+g(b)=g(a+b),\quad g(a)g(b)=g(ab) \tag{1}$$

для любых элементов a и b из S. Так как в силу взаимной однозначности отображения g для любого a' из S существует один и только один элемент a из S такой, что $g(a)=a'$, то $g(a)$ и $g(b)$ — любые элементы S', и равенства (1) действительно определяют алгебраические операции в S'.

Одновременно равенства (1) показывают, что относительно сложения и умножения S' изоморфно S и по предыдущей теореме S — кольцо. Если S — поле, то и S' — поле.

Покажем, что операции в S' для элементов R' совпадают с операциями, заданными в кольце R'. Так как f — изоморфное отображение R на R', то справедливы равенства

$$f(a)+f(b)=f(a+b),\quad f(a)f(b)=f(ab) \tag{2}$$

для любых a и b из R.

Но если в (1) $g(a)$ и $g(b)$ принадлежат R', то a, b, $a+b$ и ab принадлежат R, и по построению отображения g равенства (1) со-

впадают с равенствами (2), где сложение и умножение в левых частях означают операции, заданные в кольце R'. Этим указанное совпадение операций доказано. Значит, R' — подкольцо S'. Если R — подполе S, то по предыдущей теореме R' — также поле, т. е. подполе S. Теорема доказана.

§ 10. Расположенные кольца и поля

До сих пор мы рассматривали либо множества без всяких отношений между элементами (§ 1—4), либо множества с одним отношением порядка (§ 5), либо множества с одной или двумя алгебраическими операциями (§ 6—9). Однако важнейшую роль в математике играют числовые множества, где существуют одновременно и отношения порядка и операции. Мы рассмотрим упорядоченные кольца и поля с целесообразной связью порядка и операций.

С отношением порядка в кольце связаны понятия положительности, отрицательности и абсолютной величины элементов (см. § 7, определения 1 и 3).

Наличие операций позволяет несколько упростить введение порядка в кольце. Оказывается достаточным задать лишь порядок всех элементов относительно нуля. Далее, для сохранения обычных свойств чисел приходится наложить дополнительные требования на связь порядка с операциями. Именно:

Определение 1. *Кольцо* (в частности, *поле*) R *называется расположенным, если для его элементов определено свойство быть положительным, удовлетворяющее следующим требованиям*:

IX. *Для любого элемента* $a \in R$ *имеет место одно и только одно из трёх соотношений*: $a = 0$, a *положителен*, $-a$ *положителен.*

X. *Если* a *и* b *положительны, то* $a + b$ *и* ab *также положительны.*

Если $-a$ *положителен, то* a *называется отрицательным.*

Теорема 1. *Если в расположенном кольце* R *определить порядок, считая* $a > b$ *тогда и только тогда, когда элемент* $a - b$ *положителен, то* R *будет упорядоченным множеством* (в смысле § 5), *причём нуль будет меньше всех положительных и больше всех отрицательных элементов.*

Доказательство. Пусть a и b — элементы R. Если $a - b = 0$, то $a = b$, если $a - b$ положителен, то $a > b$, если $-(a - b) = b - a$ положителен, то $b > a$. Из свойства IX следует, что имеет место один и только один из этих трёх случаев (§ 5, свойство 1). Далее, если $a > b$ и $b > c$, то $a - b$ и $b - c$ положительны. По свойству X тогда $(a - b) + (b - c) = a - c$ положителен, т. е. $a > c$ (§ 5, свойство II). Итак, R — упорядоченное множество.

Если a положителен, то из $a = a - 0$ следует $a > 0$; если a отрицателен, то из $-a = 0 - a$ следует $0 > a$, $a < 0$.

Эта теорема показывает, что условия IX и X достаточны для введения порядка в R, причём X даёт обычную для чисел связь порядка с операциями кольца.

Теорема 2. (Законы монотонности для сложения и умножения.) *Для любых элементов a, b, c расположенного кольца R из* а) $a>b$, $a=b$, $a<b$ *следует соответственно* б) $a+c>b+c$, $a+c=b+c$, $a+c<b+c$ *и при* $c>0$ *соответственно* в) $ac>bc$, $ac=bc$, $ac<bc$, *а при* $c<0$ *— соответственно:* г) $ac<bc$, $ac=bc$, $ac>bc$.

Доказательство. Если $a>b$, то

$$(a+c)-(b+c)=a-b>0,$$

т. е. $a+c>b+c$. Если $a=b$, то $ac=bc$ по однозначности сложения. Если $a<b$, то $b>a$, и по первому случаю

$$b+c>a+c, \quad a+c<b+c.$$

Случай б) доказан.

Если $a>b$, $c>0$, то $a-b>0$, и по условию X

$$(a-b)c=ac-bc>0, \quad ac>bc.$$

Если $c<0$, то $-c>0$, и по правилу знаков при умножении [§ 7, формула (3)] имеем:

$$bc-ac=(b-a)c=[-(b-a)](-c)=(a-b)(-c)>0,$$

$$bc>ac, \quad ac<bc.$$

Итак, оба первых случая в) и г) доказаны. Остальные случаи вытекают из первых дословно, как при доказательстве б).

Справедливы также обратные теоремы, а именно:

Теорема 3. *Из*

$$a+c>b+c, \quad a+c=b+c, \quad a+c<b+c$$

следует соответственно

$$a>b, \quad a=b, \quad a<b.$$

Из

$$ac>bc, \quad ac=bc, \quad ac<bc$$

следует при $c>0$ *соответственно*

$$a>b, \quad a=b, \quad a<b,$$

а при $c<0$ *— соответственно*

$$a<b, \quad a=b, \quad a>b.$$

Доказательство. В теореме 2 посылки а) обладают тем свойством, что одна (и только одна, что сейчас неважно) из них наверное имеет место, а следствия [в каждом случае б), в), г) отдельно] — тем свойством, что они взаимно исключают друг друга. Для теорем такого рода обратные теоремы всегда верны, причём их можно доказать методом «от противного». Докажем, например, что из $ac=bc$ следует $a=b$ при $c>0$. Предположим противное, что $a\neq b$. Тогда имеет место какая-то из других посылок а) теоремы 2. Но если $a>b$, то по теореме 2 $ac>bc$, если же $a<b$, то $ac<bc$, что невозможно ввиду $ac=bc$, чем исключаются неравенства $ac>bc$ и $ac<bc$.

Следствие 1. *В расположенном кольце из* а)

$$a-b\gtreqless c-d$$

следует соответственно б)

$$a+d\gtreqless b+c,$$

и обратно.

В самом деле, прибавляя к обеим частям а) сумму $b+d$, получим б). Обратные теоремы верны, так как в а) и б) исчерпаны все случаи и они исключают друг друга.

Следствие 2. *В расположенном поле при* $bd>0$ *из* а)

$$\frac{a}{b}\gtreqless\frac{c}{d}$$

следует соответственно б)

$$ad\gtreqless bc,$$

и обратно.

Доказательство аналогично предыдущему.

Из теоремы 2 вытекают обычные для чисел правила действий с неравенствами. А именно:

Теорема 4. *Из* $a>b$ *и* $c>d$ *следует* $a+c>b+d$ *и, если все элементы* a, b, c, d *положительны, то* $ac>bd$, *если же все они отрицательны, то* $ac<bd$. *Верна также теорема, получающаяся из данной, если знаки* $>$ *и* $<$ *поменять местами.*

Доказательство. По теореме 2 из $a>b$ следует $a+c>b+c$, из $c>d$ следует $b+c>b+d$, откуда $a+c>b+d$. Точно так же доказывается, что при положительных a, b, c, d будет $ac>bd$. Пусть a, b, c, d отрицательны. Тогда из $a>b$ следует $ac<bc$ и из $c>d$ следует $bc<bd$, откуда $ac<bd$.

Как следствие из теоремы 3 получаем:

Теорема 5. *Расположенное кольцо не имеет делителей нуля* (§ 7, определение 2).

Доказательство. Пусть $ab=0$. Тогда $ab=a\cdot 0$ и по теореме 3 при $a\neq 0$, т. е. $a>0$ или $a<0$, должно быть $b=0$.

Теорема 6. *Характеристика* (см. § 8, определение 2) *расположенного поля P равна нулю.*

Доказательство. Пусть $a \neq 0$, $a \in P$. Если $a > 0$, то по свойству X для любого натурального n также $na > 0$, а так как $(-n)a = -na$, то $na \neq 0$ при любом целом n. Если $a < 0$, то $-a > 0$ и $n(-a) \neq 0$, при любом целом n. Значит, $na \neq 0$, если $a \neq 0$ и $n \neq 0$.

Теорема 7. *Сумма квадратов* (и, в частности, всякий квадрат) *конечного числа элементов расположенного кольца больше или равна нулю, причём равенство может иметь место лишь в том случае, когда все данные элементы равны нулю.*

Доказательство. Для одного элемента, если $a_1 = 0$, то $a_1^2 = 0$. Если же $a_1 \neq 0$, то или $a_1 > 0$, или $-a_1 > 0$ и тогда

$$a_1^2 = a_1 a_1 = (-a_1)(-a_1) > 0.$$

Для $n = 1$ теорема верна. Пусть она верна для n элементов. Тогда

$$\sum_{i=1}^{n+1} a_i^2 = \sum_{i=1}^{n} a_i^2 + a_{n+1}^2 \geqslant 0,$$

как сумма неотрицательных слагаемых (см. свойство X). Если одно из двух слагаемых > 0, то и сумма их > 0. Значит, в случае равенства нулю оба слагаемых равны нулю, т. е.

$$\sum_{i=1}^{n} a_i^2 = 0 \quad \text{и} \quad a_{n+1}^2 = 0.$$

Отсюда по доказанному $a_{n+1} = 0$ и по предположению индукции $a_1 = a_2 = \ldots = a_n = 0$.

Определение 2. *Абсолютной величиной элемента a расположенного кольца* (и, в частности, *поля*) *называется неотрицательный из элементов a и $-a$. Абсолютная величина элемента a обозначается через* $|a|$.

Согласно этому $|0| = 0$ и при $a \neq 0$ всегда $|a| > 0$.

Теорема 8. *Абсолютная величина суммы конечного числа элементов меньше или равна сумме абсолютных величин слагаемых. При этом равенство имеет место тогда и только тогда, когда все слагаемые неположительны или все неотрицательны. Абсолютная величина произведения конечного числа элементов равна произведению абсолютных величин сомножителей.*

Доказательство. Ограничимся случаем двух элементов, так как проведение индукции не представляет затруднений. Итак, надо доказать, что

$$|a + b| \leqslant |a| + |b|, \tag{1}$$

причём равенство имеет место тогда и только тогда, когда либо $a \geqslant 0$, $b \geqslant 0$, либо $a \leqslant 0$, $b \leqslant 0$, а также доказать, что

$$|ab| = |a| \cdot |b|. \tag{2}$$

Если $a \geqslant 0$ и $b \geqslant 0$, то также $a + b \geqslant 0$ и

$$|a + b| = a + b = |a| + |b|.$$

Если $a \leqslant 0$ и $b \leqslant 0$, то $-a \geqslant 0$, $-b \geqslant 0$ и

$$-(a + b) = (-a) + (-b) \geqslant 0,$$

откуда

$$|a + b| = -(a + b) = (-a) + (-b) = |a| + |b|.$$

Итак, в этих двух случаях (1) имеет место при знаке $=$. По симметрии a и b в (1) из двух оставшихся случаев $a > 0$, $b < 0$ и $a < 0$, $b > 0$ достаточно разобрать лишь первый. По теореме 2, прибавляя a к неравенству $b < -b$, получим:

$$a + b < a + (-b) = |a| + |b|.$$

Точно так же, прибавляя $-b$ к неравенству $-a < a$, получим:

$$-(a + b) = (-a) + (-b) < a + (-b) = |a| + |b|.$$

Но $|a + b|$ совпадает либо с $a + b$, либо с $-(a + b)$. Поэтому

$$|a + b| < |a| + |b|.$$

Итак, в этих двух случаях (1) имеет место при знаке $<$.

Равенство (2), очевидно, выполнено, если хотя бы один из элементов a, b равен нулю. Остаётся разобрать три случая:

1) $a > 0$, $b > 0$. По свойству X $ab > 0$ и $|ab| = ab = |a| \cdot |b|$.

2) $a < 0$, $b < 0$, $-a > 0$, $-b > 0$, $(-a)(-b) > 0$ и по правилу знаков (3) из § 7

$$|ab| = |(-a)(-b)| = (-a)(-b) = |a| \cdot |b|.$$

3) $a > 0$, $b < 0$, $-b > 0$, $a(-b) > 0$,

$$|ab| = |-ab| = |a(-b)| = a(-b) = |a| \cdot |b|.$$

Из неравенства (1) следует

$$\big|\,|a| - |b|\,\big| \leqslant |a \pm b| \leqslant |a| + |b| \tag{3}$$

для любых элементов a и b расположенного кольца R. В самом деле, так как $a + b = a - (-b)$ и $|b| = |-b|$, то достаточно

доказать (3) для случая разности $a-b$. Но из $a=(a-b)+b$ и $b=(b-a)+a$ по (1) найдём: $|a|\leqslant|a-b|+|b|$ и

$$|b|\leqslant|b-a|+|a|=|a-b|+|a|,$$

откуда

$$|a|-|b|\leqslant|a-b| \quad \text{и} \quad |b|-|a|\leqslant|a-b|;$$

поэтому

$$\big|\,|a|-|b|\,\big|\leqslant|a-b|=|a+(-b)|\leqslant|a|+|b|.$$

Замечание. Точно так же известные из элементарной алгебры правила сравнения и действий над «относительными числами» через сравнение и действия над их абсолютными величинами остаются справедливыми для любого расположенного кольца R.

Именно, положительный элемент кольца R больше отрицательного, что ясно из сравнения с нулём. Из двух положительных элементов тот больше, абсолютная величина которого больше, ибо положительные элементы совпадают с их абсолютными величинами. Из двух отрицательных элементов тот больше, абсолютная величина которого меньше. В самом деле, если a и b отрицательны, то $a-b=(-b)-(-a)=|b|-|a|$ и поэтому $a>b$ тогда и только тогда, когда $|a|<|b|$.

Если по симметрии с обозначением элемента, противоположного a, через $-a$ обозначить сам элемент a через $+a$, то каждый элемент можно выразить через его абсолютную величину так: $a=\pm|a|$, где знак $+$ берётся для положительного и $-$ для отрицательного элемента a. В этом смысле можно говорить о знаке данного элемента. Тогда имеют место следующие правила действий.

Чтобы сложить два элемента одного знака, надо сложить их абсолютные величины и поставить тот знак, который имели слагаемые. В самом деле, если $a>0$ и $b>0$, то это очевидно; если же $a<0$ и $b<0$, то $a+b=(-|a|)+(-|b|)=-(|a|+|b|)$.

Чтобы сложить два элемента разных знаков, надо из большей абсолютной величины вычесть меньшую (при равенстве абсолютных величин сумма равна нулю) и поставить знак того слагаемого, у которого абсолютная величина больше. Пусть $a>0$ и $b<0$. Если $|a|>|b|$, то

$$a+b=a-(-b)=+(|a|-|b|).$$

Если же $|a|<|b|$, то

$$a+b=-(-b-a)=-(|b|-|a|).$$

Чтобы из одного элемента вычесть другой, надо к первому элементу прибавить элемент, противоположный второму. Это верно даже для любых колец.

Чтобы умножить (разделить) один элемент на другой, надо абсолютную величину первого элемента умножить (разделить) на абсолютную величину второго и поставить знак $+$, если знаки данных элементов одинаковы, и знак $-$, если различны. Для умножения это следует из правила знаков в любом кольце [§ 7, (3)], ибо $ab=(\pm|a|)\cdot(\pm|b|)$, а для деления (если оно выполнимо) выводится отсюда так: если $\frac{a}{b}=c$, то $a=bc$, $|a|=|b|\cdot|c|$, откуда $\frac{|a|}{|b|}=|c|$.

При умножении на положительный элемент знак сохраняется, а на отрицательный — меняется. Поэтому из $a=bc$ следует, что при одинаковых знаках a и b частное c положительно, а при разных знаках отрицательно.

Мы видим, таким образом, что обычные правила оперирования с неравенствами и абсолютными величинами верны не только для чисел, но и для элементов любых расположенных колец. Эти правила являются следствием аксиом I — VI, IX и X.

Есть, однако, одно важное свойство чисел, которое уже не переносится на любые расположенные кольца. Это — выполнение так называемой аксиомы Архимеда, согласно которой, складывая само с собой любое данное положительное число (как бы мало оно ни было) достаточное число раз, мы можем получить число, превосходящее любое (сколь угодно большое) данное число. Поэтому кольца, обладающие аналогичным свойством, нуждаются в особом определении.

Определение 3. *Кольцо* (в частности, *поле*) *называется архимедовски расположенным, если оно обладает свойством*:

XI. (Аксиома Архимеда.) *Для любых элементов a и b кольца, где $b>0$, существует натуральное число n такое, что $nb>a$.*

В случае поля достаточно выполнения этого условия лишь для единицы поля e, т. е. свойство XI эквивалентно свойству

XI′. *Для любого элемента a поля существует натуральное число n такое, что $ne>a$.*

Действительно, если $b>0$, то существует натуральное число n, для которого $ne>\frac{a}{b}$, и, умножая на $b>0$, получим: $nb>a$.

Пример 1. Кольцо целых, поле рациональных и поле действительных чисел архимедовски расположены (доказательства даны в соответствующих главах).

Пример 2. Пусть R есть кольцо многочленов

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$$

с рациональными коэффициентами (при обычных операциях сложения

и умножения). Будем считать многочлен $f(x)$ положительным, если его старший коэффициент a_n положителен. Легко видеть, что аксиомы IX и X определения (1) выполняются, т. е. R — расположенное кольцо. Но хотя $1 > 0$, $n \cdot 1 = n < x$ при любом натуральном (даже при любом рациональном) n, так как $x - n > 0$. Значит, R — неархимедовски расположенное кольцо. Алгебраические дроби вида $\frac{f(x)}{g(x)}$, где $f(x)$ и $g(x)$ — многочлены кольца R, образуют поле P. Читателю предлагается доказать, что поле P будет расположено, если дробь $\frac{f(x)}{g(x)}$ считать положительной, когда $f(x)$ и $g(x)$ имеют одинаковые знаки при указанном выше расположении R. Так как снова $n \cdot 1 < x$, то P — неархимедовски расположенное поле.

ГЛАВА III

НАТУРАЛЬНЫЕ ЧИСЛА

§ 11. Аксиомы натуральных чисел

Аксиоматическое построение данной теории начинается (см. § 9) с перечисления основных отношений (принимаемых без определения) и основных свойств или аксиом (принимаемых без доказательства), которым удовлетворяют данные отношения. При аксиоматическом построении натуральных чисел вводится одно основное отношение и четыре аксиомы, а именно:

Определение 1. *Натуральными числами называются элементы всякого непустого множества N, в котором для некоторых элементов a, b существует отношение «b следует за a»* (число, следующее за a, будем обозначать через a'), *удовлетворяющее следующим аксиомам:*

I. *Существует число* 1, *не следующее ни за каким числом, т. е.* $a' \neq 1$ *для любого числа* a[1]).

II. *Для любого числа a существует следующее число a' и притом только одно, т. е. из* $a = b$ *следует* $a' = b'$.

III. *Любое число следует не более чем за одним числом, т. е. из* $a' = b'$ *следует* $a = b$.

IV. (Аксиома индукции.) *Любое множество M натуральных чисел, обладающее свойствами:*

А) 1 *принадлежит M,*

Б) *если число a принадлежит M, то следующее число a' также принадлежит M,*

содержит все натуральные числа, т. е. совпадает с N.

Приведённая здесь аксиоматика натуральных чисел представляет собой лишь несущественное изменение системы аксиом, предложенной в 1891 г. итальянским математиком и логиком Пеано.

Может показаться, что наше определение натуральных чисел плохо тем, что согласно ему натуральными числами называются

---

[1]) Как всегда, знак $=$ обозначает совпадение, а знак $\neq$ — различие элементов множества.

элементы всякого множества N, обладающего перечисленными свойствами.

Действительно, возможны различные множества, удовлетворяющие определению 1, но все они изоморфны относительно основного отношения «b следует за a» (см. определение 1 из § 9) и поэтому обладают совершенно одинаковыми свойствами, касающимися этого отношения, если только эти свойства вытекают из аксиом I — IV.

Отложив до конца главы (§ 17) доказательство упомянутого изоморфизма и другие вопросы, касающиеся самой системы аксиом, займёмся теми следствиями, которые из неё проистекают.

Поясним, прежде всего, смысл аксиомы индукции. Обычное доказательство по индукции состоит в следующем. Пусть надо доказать некоторую теорему, в формулировке которой участвует натуральное число n (как, например, в формуле бинома Ньютона). Тогда доказывают эту теорему, во-первых, для $n=1$ и, во-вторых, для числа $n+1$, предполагая, что она верна для числа n. После этого теорема считается доказанной для любого числа n. То, что теорема действительно доказана для любого n, обычно обосновывается так: теорема верна для 1, а значит, и для 2, раз она верна для 2, значит, верна и для 3; раз для 3, значит, и для 4 и т. д. Но что значит это «и т. д.»? Можем ли мы, рассуждая так, перебрать все натуральные числа? Разумеется, нет, так как этих чисел бесконечно много. Аксиома индукции IV и служит как раз формальным средством доказательства такого рода теорем сразу для всей бесконечной совокупности натуральных чисел. А именно, верна такая теорема:

Теорема 1. (Теорема о законности индуктивных доказательств.) *Если некоторая теорема T, формулировка которой содержит натуральное число n, доказана для числа 1 и в предположении, что она верна для числа n, доказана для следующего числа n'* [1]*, то эта теорема верна для любого числа n.*

Доказательство. Пусть M есть множество тех натуральных чисел, для которых верна рассматриваемая теорема T. Тогда

А) число 1 входит в M, так как для 1 теорема T доказана;

Б) пусть число n принадлежит M; это значит, для числа n теорема T верна. Но в таком случае теорема T доказана, т. е. также верна и для следующего числа n', а это значит, что число n' также принадлежит M. Итак, множество M обладает свойствами А) и Б) аксиомы IV. В силу этой аксиомы оно должно содержать все натуральные числа, что означает (по самому определению множества M), что теорема T верна для любого натурального числа n. Этим теорема 1 доказана.

---

[1]) Для того чтобы считать $n'=n+1$, надо ещё определить сложение натуральных чисел.

Определение 2. *Если b следует за a, то говорят, что a предшествует b.*

Согласно аксиоме I число 1 не имеет предшествующего. Но это — единственное число с таким свойством.

Теорема 2. *Любое число $a \neq 1$ имеет предшествующее число и притом только одно.*

Доказательство. Пусть M — множество, содержащее 1 и все числа, имеющие хотя бы одно предшествующее число.

А) 1 принадлежит M, Б) если a принадлежит M, то и a' также принадлежит M, ибо a' имеет предшествующее число a (предположение, что a принадлежит M, здесь даже излишне). По аксиоме IV M содержит все числа. Значит, любое число $a \neq 1$ имеет по крайней мере одно предшествующее. Единственность предшествующего числа следует из аксиомы III, согласно которой любое число имеет не более одного предшествующего.

Теорема 3. *Если числа, следующие за данными числами, различны, то и данные числа различны, т. е. из $a' \neq b'$ следует $a \neq b$.*

Доказательство. По аксиоме II из $a = b$ следует $a' = b'$.

Теорема 4. *Если данные числа различны, то и следующие за ними различны, т. е. из $a \neq b$ следует $a' \neq b'$.*

Доказательство. По аксиоме III из $a' = b'$ следует $a = b$.

Теорема 5. *Любое число отлично от следующего за ним числа, т. е. $a \neq a'$ для любого a.*

Доказательство. Пусть M — множество чисел, для которых теорема верна.

А) По аксиоме I $1' \neq 1$. Следовательно, 1 принадлежит M.

Б) Если a принадлежит M, то $a' \neq a$. Значит, по теореме 4 также $(a')' \neq a'$, т. е. a' принадлежит M. По аксиоме IV M содержит все числа, т. е. $a \neq a'$ для любого a.

§ 12. Сложение

Определение. *Сложением натуральных чисел называется такое соответствие, которое с каждой парой натуральных чисел a и b сопоставляет одно и только одно натуральное число $a + b$, обладающее следующими свойствами:*

1) $a + 1 = a'$ *для любого a,*

2) $a + b' = (a + b)'$ *для любых a и b.*

Числа a и b называются слагаемыми, а число $a + b$ — суммой [1].

Сразу возникает вопрос, существует ли такое соответствие, и если да, то будет ли оно единственным. Приведённое определение является примером так называемого индуктивного определения. Пусть

[1]) Сложение является, таким образом, частным случаем более общего понятия алгебраической операции (см. § 6, определение 1) или ещё более общего понятия функции (см. § 3, определение 1).

выбрано определённое число a. Тогда условия 1) и 2) определяют число $a+1$ и число $a+b'$, если уже определено число $a+b$. Поэтому на основании аксиомы индукции IV можно, казалось бы, считать число $a+b$ определённым для любого b, а так как a выбиралось произвольно, то и для любых a и b. Так полагали автор аксиоматики натуральных чисел Пеано и его ученики. Такое изложение принято в большинстве математических книг. Однако в этом рассуждении имеется ошибка. В самом деле, каждый раз, применяя аксиому индукции, мы должны вполне точным образом определить то множество M, для которого надо доказать свойства А) и Б). В доказанной выше теореме 1 (§ 11) множество M состоит из тех натуральных чисел, для которых верна некоторая теорема T о натуральном числе n. Нам удалось доказать, что это множество обладает свойствами А) и Б), что и доказывало теорему T. Этим снимается то возражение, что при доказательстве теоремы T для $n+1$ мы предполагаем её уже доказанной для n, хотя она ещё только доказывается. Мы пока и не пользуемся тем, что теорема T верна для n, а доказываем лишь предложение в условной форме: «Если теорема T верна для n, то она верна и для $n+1$», что соответствует условной форме свойства Б).

Попробуем теперь выяснить, к какому множеству M надо применить аксиому IV в случае определения сложения? Можно ли сказать, что при выбранном a множество M состоит из тех b, для которых число $a+b$ определено? Нельзя, потому что мы ещё только хотим доказать, что число $a+b$ определено свойствами 1) и 2). В этом и состоит как раз отличие индуктивного определения от индуктивного доказательства, где множество M чисел, для которых теорема T верна, имеет вполне определённый смысл независимо от того, доказана эта теорема T или нет. Слова «при данном a число $a+b$ со свойствами 1) и 2) определено» имеют лишь такой точный смысл: «при данном a существует соответствие, сопоставляющее с числом b число $a+b$ и обладающее свойствами 1) и 2)», но это утверждение касается не одного, а сразу всех чисел b и потому его нельзя доказать индукцией по b простой ссылкой на свойства 1) и 2). Зато это утверждение касается одного определённого числа a, и можно пытаться доказать его индукцией по a (что и будет сделано ниже). Заметим, что мы утверждаем ошибочность доказательства индукцией по b того, что условия 1) и 2) определяют число $a+b$, но отнюдь не ошибочность самого этого утверждения. Индуктивные определения законны, что можно доказать, опираясь только на понятие о порядке натуральных чисел (см. § 15). Понятие же порядка будет нами введено (см. § 14) на основе сложения. Таким образом, вопрос о существовании сложения приходится решать иным путём.

Теорема 1. *Сложение натуральных чисел существует и притом только одно, т. е. существует одно и только одно соот-*

ветствие, сопоставляющее с любыми числами a и b число $a+b$ так, что

1) $a+1=a'$ *для любого* a,

2) $a+b'=(a+b)'$ *для любых* a *и* b. *Иными словами, сложение всегда выполнимо и однозначно.*

Доказательство. а) Сначала докажем, что при данном a существует не более чем одно соответствие, сопоставляющее с каждым числом b число x_b и обладающее свойствами: $x_1=a'$, $x_{b'}=(x_b)'$ для любого b. Пусть y_b — любое соответствие с теми же свойствами, т. е. $y_1=a'$, $y_{b'}=(y_b)'$ для любого b. Пусть M — множество тех чисел b, для которых $x_b=y_b$.

А) $x_1=a'=y_1$; 1 принадлежит M.

Б) Если b принадлежит M, то $x_b=y_b$, значит, по аксиоме II $(x_b)'=(y_b)'$, следовательно, $x_{b'}=(x_b)'=(y_b)'=y_{b'}$, т. е. b' принадлежит M. По аксиоме IV M содержит все натуральные числа, т. е. $x_b=y_b$ для любого b. Единственность сложения доказана при данном a. Но по произвольности a она доказана для любых a и b.

б) Покажем теперь, что при данном a существует [и согласно а) только одно] соответствие, сопоставляющее с каждым b число $a+b$ и обладающее свойствами: $a+1=a'$, $a+b'=(a+b)'$ для любого b (при данном a). Пусть M — множество тех чисел a, для которых такое соответствие существует [и по а) только одно].

А) При $a=1$ положим для любого b, что $a+b=b'$. Это соответствие обладает нужными свойствами, так как

$$a+1=1'=a', \quad a+b'=(b')'=(a+b)'.$$

Значит, 1 принадлежит M.

Б) Если a принадлежит M, то число $a+b$ определено и обладает свойствами: $a+1=a'$, $a+b'=(a+b)'$. Числу b поставим в соответствие число $a'+b=(a+b)'$. Это соответствие обладает нужными свойствами для a', так как

$$a'+1=(a+1)'=(a')', \quad a'+b'=(a+b')'=[(a+b)']'=(a'+b)'.$$

Значит, число a' принадлежит M. По аксиоме IV M содержит все натуральные числа, т. е. для любого a существует соответствие, сопоставляющее с каждым b число $a+b$ и обладающее свойствами

$$a+1=a', \quad a+b'=(a+b)'$$

для данного a и любого b. Но число a является произвольным. Следовательно, доказано существование и единственность соответствия, сопоставляющего с любыми a и b число $a+b$ и обладающее свойствами 1) и 2). Теорема доказана.

Теорема 2. (Закон ассоциативности сложения.)

$$(a+b)+c=a+(b+c).$$

Доказательство. Пусть выбраны числа a и b и пусть M — множество тех чисел c, для которых равенство справедливо.

А) $(a+b)+1=(a+b)'=a+b'=a+(b+1)$;

1 принадлежит M. Б) Если c принадлежит M, то $(a+b)+c=a+(b+c)$, откуда

$$(a+b)+c'=[(a+b)+c]'=[a+(b+c)]'=a+(b+c)'=a+(b+c'),$$

т. е. c' принадлежит M. По аксиоме IV равенство $(a+b)+c=a+(b+c)$ справедливо для любых a, b и c.

Теорема 3. (Закон коммутативности сложения.)

$$a+b=b+a.$$

Доказательство. а) Докажем, что $a+1=1+a$ индукцией по a. Пусть M — множество тех a, для которых это верно. А) 1, очевидно, принадлежит M. Б) Если a принадлежит M, то $a+1=1+a$. Тогда

$$a'+1=(a+1)+1=(1+a)+1=(1+a)'=1+a',$$

т. е. a' принадлежит M. По аксиоме IV доказано, что $a+1=1+a$.

б) Докажем индукцией по b, что $a+b=b+a$. Пусть M — множество тех b, для которых это верно при данном a. А) По доказанному в а) 1 принадлежит M. Б) Если b принадлежит M, то $a+b=b+a$. Тогда, используя теорему 2, находим:

$$a+b'=(a+b)'=(b+a)'=b+a'=b+(a+1)=b+(1+a)=(b+1)+a=b'+a,$$

т. е. b' принадлежит M. По аксиоме IV теорема доказана.

Теорема 4.

$$a+b\neq b.$$

Доказательство. Теорема верна для $b=1$, ибо $a+1=a'\neq 1$ по аксиоме I. Если $a+b\neq b$, то по теореме 4 из § 11 также

$$a+b'=(a+b)'\neq b'.$$

Теорема 5. *Для любых чисел a и b имеет место один и только один из случаев*: 1) $a=b$; 2) *существует число k такое, что* $a=b+k$; 3) *существует число l такое, что* $b=a+l$.

Доказательство. Из теоремы 4 следует, что имеет место не более чем один из этих случаев, так как, очевидно, 1) и 2), а также 1) и 3) не могут иметь места одновременно. Если бы имели место 2) и 3), то

$$a=b+k=(a+l)+k=a+(l+k),$$

что снова противоречит теореме 4. Докажем, что хотя бы один из этих случаев всегда имеет место.

Пусть выбрано число a, и M — множество тех b, для каждого из которых при данном a имеет место 1), 2) или 3). А) Если $a=1$, то имеем случай 1) для $b=1$. Если $a\neq 1$, то по теореме 2 из § 11 $a=k'=k+1=1+k$, т. е. имеем случай 2) для $b=1$. Итак, 1 принадлежит M. Б) Пусть b принадлежит M. Тогда или $a=b$, и следовательно, $b'=b+1=a+1$, т. е. случай 3) для b'; или $a=b+k$, и если $k=1$, то $a=b+1=b'$, т. е. случай 1) для b'; если же $k\neq 1$, то $k=m'$ и

$$a=b+m'=b+(m+1)=b+(1+m)=(b+1)+m=b'+m,$$

т. е. случай 2) для b'; или $b=a+l$ и

$$b'=(a+l)'=a+l',$$

т. е. случай 3) для b'. Во всех случаях b' принадлежит M. Теорема доказана.

Пользуясь этой теоремой, можно было бы уже теперь дать определение порядка и доказать основные его свойства (см. § 14), но мы рассмотрим сначала свойства умножения, чтобы затем сразу рассмотреть связь понятия порядка с обеими основными операциями.

Задача. Определив натуральные числа

$$2=1',\quad 3=2',\quad 4=3',\quad 5=4',\quad 6=5',$$

доказать на основании определения суммы, что

$$1+1=2,\quad 1+2=3,\quad 2+2=4,\quad 2+3=5,\quad 2+4=3+3=6.$$

§ 13. Умножение

Определение. *Умножением натуральных чисел называется такое соответствие, которое с каждой парой натуральных чисел a и b сопоставляет одно и только одно натуральное число ab* (или $a\cdot b$ или $a\times b$), *обладающее следующими свойствами*:

1) $a\cdot 1=a$ *для любого* a;

2) $ab'=ab+a$ *для любых* a *и* b.

Число a называется множимым, b — множителем, оба числа a и b называются также сомножителями, а число ab — произведением.

На первый взгляд может показаться странным, зачем давать это индуктивное определение, вместо того чтобы остаться при всем известном школьном определении произведения ab как суммы b слагаемых, каждое из которых равно множимому a. Но что означает выражение «b слагаемых», где b выступает в роли количественного числительного? Количество слагаемых имеет лишь один точный смысл, именно, — это мощность некоторого множества

(см. § 3, определение 4). Правда, для конечных множеств (с которыми мы и имеем дело при определении умножения) мы дали другое определение «числа элементов» (см. § 4, определение 3) и доказали, что оно совместимо с понятием числа элементов как мощности множества, но мы существенно использовали при этом понятие отрезка $|1, n|$ натурального ряда как множества натуральных чисел, не превосходящих n. Это понятие предполагает уже установленным порядок во множестве натуральных чисел; правда, мы могли бы определить порядок до умножения и установить с помощью определения 3 из § 4 соответствие, позволяющее отождествить натуральные числа с мощностями конечных множеств. Это дало бы натуральным числам количественный характер. Однако арифметика натуральных чисел в этом не нуждается. Всю её можно построить, не используя понятия о мощности, а лишь на основе определения 1. Построенные таким путём натуральные числа называют *порядковыми числами* в отличие от мощностей, называемых *количественными числами*.

Для того чтобы теория натуральных чисел не осталась пустой логической игрой, а стала тем основным орудием практической деятельности человека, которым она на самом деле является, необходимо установить соответствие между мощностями конечных множеств и независимо от них построенными порядковыми натуральными числами, придав им тем самым количественный смысл. В этом и состоит значение определения 3 и теоремы 2, на которой оно основано, приведённых в § 4.

Относительно определения умножения сохраняют силу все замечания, которые были сделаны в предыдущем параграфе по поводу определения сложения. В частности, из него ещё неясно, что соответствие с этими свойствами существует. Поэтому большое принципиальное значение имеет следующая теорема, аналогичная теореме 1 из § 12.

Теорема 1. *Умножение натуральных чисел существует и притом только одно. Иными словами, умножение всегда выполнимо и однозначно.*

Доказательство. а) Сначала докажем, что при данном a существует не более чем одно соответствие, сопоставляющее с каждым числом b число x_b и обладающее свойствами $x_1 = a$, $x_{b'} = x_b + a$ для любого b. Пусть y_b — любое соответствие с теми же свойствами и M — множество тех b, для которых $x_b = y_b$.

А) $x_1 = a = y_1$; 1 принадлежит M. Б) Если b принадлежит M, то $x_{b'} = x_b + a = y_b + a = y_{b'}$; b' принадлежит M. По аксиоме IV $x_b = y_b$ для любого b. Единственность умножения доказана при данном a, а по произвольности a она доказана для любых a и b.

б) Покажем теперь, что при данном a существует [и согласно а) только одно] соответствие, сопоставляющее с каждым b число ab и обладающее свойствами $a \cdot 1 = a$, $ab' = ab + a$ для любого b (при

данном a). Пусть M — множество тех чисел a, для которых такое соответствие существует [и по a) только одно].

А) При $a=1$ положим для любого b, что $ab=b$. Это соответствие обладает нужными свойствами, так как

$$a\cdot 1=1=a,\quad ab'=b'=b+1=ab+a;$$

1 принадлежит M.

Б) Если a принадлежит M, то любому b соответствует ab, причём $a\cdot 1=a$, $ab'=ab+a$. Для a' строим такое соответствие: числу b соответствует число $a'\cdot b=ab+b$. Оно обладает нужными свойствами, так как

$$a'\cdot 1=a\cdot 1+1=a+1=a',$$
$$a'\cdot b'=ab'+b'=(ab+a)+b'=ab+(a+b')=ab+(a+b)'=$$
$$=ab+(b+a)'=ab+(b+a')=(ab+b)+a'=a'\cdot b+a';$$

a' принадлежит M. Соответствие с нужными свойствами построено при любом a для каждого b, т. е. для любых a и b. Теорема доказана.

Теорема 2. (Правый закон дистрибутивности.)

$$(a+b)c=ac+bc.$$

Доказательство. Для данных a и b применим индукцию по c.

А) $(a+b)\cdot 1=a+b=a\cdot 1+b\cdot 1$. Для $c=1$ теорема верна.
Б) Если теорема верна для c, то $(a+b)c=ac+bc$.

Используя ассоциативность и коммутативность сложения, находим:

$$(a+b)c'=(a+b)c+(a+b)=(ac+bc)+(a+b)=$$
$$=(ac+a)+(bc+b)=ac'+bc',$$

т. е. теорема верна и для c'. По аксиоме IV теорема доказана.

Теорема 3. (Закон коммутативности умножения.)

$$ab=ba.$$

Доказательство. а) Индукцией по b докажем теорему при $a=1$, т. е. $1\cdot b=b\cdot 1$; M — множество b с этим свойством.

А) 1 принадлежит M. Б) Если $1\cdot b=b\cdot 1$, то

$$1\cdot b'=1\cdot b+b=b\cdot 1+1=b+1=b'=b'\cdot 1;$$

b' принадлежит M.

б) Индукцией по a докажем, что $ab=ba$ при данном b; M — множество a с $ab=ba$.

А) Согласно а) 1 принадлежит M.

Б) Если a принадлежит M, то $ab = ba$. Тогда, используя предыдущую теорему, найдём:

$$a' \cdot b = (a + 1)\, b = ab + 1 \cdot b = ba + b \cdot 1 = ba + b = ba';$$

a' принадлежит M.

Теорема 4. (Левый закон дистрибутивности.)

$$c(a + b) = ca + cb.$$

Доказательство следует из теорем 2 и 3.

Теорема 5. (Закон ассоциативности умножения.)

$$(ab)\, c = a\,(bc).$$

Доказательство. Пусть даны a и b; M — множество тех c, для которых равенство имеет место.

А) $(ab) \cdot 1 = ab = a\,(b \cdot 1)$; 1 принадлежит M.

Б) Если c принадлежит M, то $(ab)\, c = a\,(bc)$. Тогда, используя теорему 4, найдём:

$$(ab)\, c' = (ab)\, c + ab = a\,(bc) + ab = a\,(bc + b) = a\,(bc');$$

c' принадлежит M. Теорема доказана.

Задача. Определив попрежнему $2 = 1'$, $3 = 2'$, $4 = 3'$, ..., доказать равенство $2 \cdot 2 = 4$, $3 \cdot 2 = 6$.

§ 14. Порядок

При определении натуральных чисел (§ 11, определение 1) мы исходили из одного основного отношения «b следует за a». Уже сам выбор слова «следует» указывает на связь этого основного отношения с понятием порядка, введённым в § 5 для любых множеств. Правда, аксиомы II и III показывают, что отношение «следует» для чисел отличается от одноимённого отношения порядка. Оно связывает каждый элемент лишь с двумя «соседними», так как по аксиоме II за каждым числом следует только одно, а по аксиоме III каждое число следует не более чем за одним числом. Но можно определить отношение порядка для любых натуральных чисел, совпадающее с уже заданным отношением «следует» между a и a'. Для этого нового отношения мы будем пользоваться словом «больше».

Определение. *Если для данных чисел a и b существует число k такое, что $a = b + k$, то говорят, что a больше b, b меньше a и пишут: $a > b$, $b < a$. Если $a > b$ или $a = b$, то пишут: $a \geqslant b$. Если $a < b$ или $a = b$, то пишут: $a \leqslant b$.*

Теорема 1. а) *Для любых чисел a, b имеет место одно и только одно из трёх соотношений: $a = b$, $a > b$, $b > a$.* б) *Из $a > b$, $b > c$ следует $a > c$. Иными словами, множество N натуральных чисел с только что определённым отношением «больше» является упорядоченным множеством в смысле определения* 1 § 5

(то, что в § 5 основное отношение обозначалось знаком $<$, значения не имеет).

Доказательство. Утверждение а) является лишь перефразировкой теоремы 5 из § 12. Утверждение б) доказывается так: если $a>b$, $b>c$, то $a=b+k$, $b=c+l$, откуда

$$a=b+k=(c+l)+k=c+(l+k),$$

т. е.

$$a>c.$$

Отношение «больше» совпадает в частном случае соседних чисел с отношением «следует», так как $a'=a+1$, т. е. $a'>a$.

Что касается связи порядка с операциями сложения и умножения, то для натуральных чисел сохраняют силу многие из теорем, доказанных в § 10 для упорядоченных колец. Так как, однако, натуральные числа, как мы увидим, не образуют кольца, то эти теоремы (если только они опирались на свойства кольца) приходится доказывать заново.

Теорема 2. (Законы монотонности сложения и умножения.) *Из* а) $a \gtreqless b$ *следует соответственно*

$$\text{б)}\ a+c \gtreqless b+c, \quad \text{в)}\ ac \gtreqless bc.$$

Доказательство. 1) Пусть $a>b$. Тогда $a=b+k$,

$$a+c=(b+k)+c=c+(b+k)=(c+b)+k=(b+c)+k,$$

откуда $a+c>b+c$, а также $ac=(b+k)c=bc+kc>bc$.

2) Пусть $a=b$. Тогда по однозначности сложения и умножения также $a+c=b+c$ и $ac=bc$.

3) Пусть $a<b$, тогда $b>a$, и по доказанному в 1) $b+c>a+c$, $bc>ac$, откуда $a+c<b+c$, $ac<bc$.

Справедливы утверждения, обратные теореме 2.

Теорема 3. *Из* $a+c \gtreqless b+c$ *или из* $ac \gtreqless bc$ *следует соответственно* $a \gtreqless b$.

Доказательство. Так как посылки и следствия в теореме 2 исчерпывают все возможности и взаимно исключают друг друга, то обратные теоремы также верны (см. доказательство теоремы 3 из § 10).

Из теоремы 2 уже дословным повторением доказательства теоремы 4 из § 10 получаются известные правила оперирования с неравенствами:

Теорема 4. *Из* $a \gtreqless b$, $c \gtreqless d$ *следует соответственно* $a+c \gtreqless b+d$, $ac \gtreqless bd$.

Теорема 5. *Единица — наименьшее из натуральных чисел, т. е.* $a \geqslant 1$ *для любого* a.

Доказательство. Если $a \neq 1$, то по теореме 2 (§ 11) $a = b' = b + 1 > 1$.

Теорема 6. *Во множестве натуральных чисел выполнена аксиома Архимеда* (§ 10, определение 3), *т. е. для любых* a и b *существует* c, *для которого* $bc > a$.

Доказательство. Достаточно взять $c > a$, так как из $b \geqslant 1$ ввиду теорем 2 и 4 следует $bc > a \cdot 1 = a$.

Теорема 7. *При установленном порядке натуральных чисел числа* a и $a + 1$ *являются соседними* (§ 5), *т. е. не существует числа* b *такого, что* $a + 1 > b > a$ *и, значит, из* $b > a$ *следует* $b \geqslant a + 1$ *и из* $b < a + 1$ *следует* $b \leqslant a$.

Доказательство. Если $b > a$, то $b = a + k$. По теореме 5 $k \geqslant 1$. По теореме 2 $a + k \geqslant a + 1$, т. е. $b \geqslant a + 1$. По теореме 1 этим исключается соотношение $a + 1 > b$. Теорема доказана.

Очень часто применяется следующая:

Теорема 8. *Любое непустое множество* A *натуральных чисел содержит наименьшее число, т. е. меньшее всех других чисел данного множества.*

Доказательство. Пусть M — множество тех чисел a, которые равны или меньше, чем все числа множества A. По теореме 5 1 принадлежит M. Не все числа принадлежат M, так как если b принадлежит множеству A, то число $a = b + 1 > b$ и не принадлежит M. Поэтому множество M должно содержать такое число a, для которого число $a + 1$ не принадлежит M (иначе по аксиоме IV M содержало бы все числа). Так как a принадлежит M, то для любого b из A должно быть $a \leqslant b$. Число a принадлежит A, так как иначе для любого b из A будет $a < b$ и по теореме 7 $a + 1 \leqslant b$, т. е. $a + 1$ принадлежит M, что противоречит выбору числа a.

На этой теореме основана вторая форма индуктивного доказательства.

Теорема 9. (Сравнить с теоремой 1 § 11.) *Если некоторая теорема* T *доказана для числа* 1 *и в предположении, что она верна для всех чисел, меньших числа* n, *где* $n > 1$, *доказана для* n, *то она верна для любого* n.

Доказательство. Если теорема T верна не для всех чисел, то множество M чисел, для которых она неверна, непусто. По теореме 8 множество M содержит наименьшее число n. Раз n принадлежит M, то для n теорема T неверна и $n > 1$. Но n — наименьшее число M, стало быть теорема T верна для всех чисел, меньших n, и должна быть верна для n, что невозможно.

После введения порядка для натуральных чисел первая форма индуктивного доказательства, т. е. теорема 1 из § 11, допускает следующие видоизменения:

Теорема 10. *Если некоторая теорема T доказана для какого-либо натурального числа k и если в предположении, что она верна для числа $n \geqslant k$, она доказана для числа $n+1$, то эта теорема T верна для любого натурального числа $n \geqslant k$.*

Доказательство. Предположим, что теорема T верна не для всех чисел $n \geqslant k$. Тогда множество A тех чисел $n \geqslant k$, для которых теорема T неверна, непусто и по теореме 8 содержит наименьшее число $l \geqslant k$, и для l теорема T неверна. Поэтому $l > k$. По теореме 5 $l \neq 1$ и потому имеет предшествующее число n (§ 11, теорема 2), т. е. число n, для которого $n' = n+1 = l$, причём $n \geqslant k$, ибо если $n < k$, то по теореме 7 $l = n+1 \leqslant k$.

Из $l = n+1$ следует $n < l$. Поэтому n не принадлежит множеству A, т. е. для n теорема T верна. Но тогда она верна и для числа $n+1 = l$. Полученное противоречие доказывает нашу теорему.

Аналогичное видоизменение допускает и вторая форма индуктивного доказательства (т. е. теорема 9), а именно:

Теорема 11. *Если некоторая теорема T, касающаяся натурального числа, доказана для числа k и в предположении, что она верна для всех чисел a с условием $k \leqslant a < n$, доказана для числа n, то эта теорема T верна для любого числа $n \geqslant k$.*

Доказательство аналогично доказательству теоремы 10 и предоставляется читателю.

Справедливо ещё следующее положение, дополняющее теорему 8:

Теорема 12. *Любое непустое и ограниченное сверху множество A натуральных чисел содержит наибольшее число* (при этом под множеством, ограниченным сверху, понимается множество, все числа которого меньше одного и того же натурального числа k).

Доказательство. Пусть B есть множество натуральных чисел, не меньших чем числа множества A. Так как A ограничено сверху, то B непусто. По теореме 8 B содержит наименьшее число b. По определению B имеем $b \geqslant a$ для любого a из A. Покажем, что число b принадлежит A и, следовательно, является наибольшим числом в A. Если b не принадлежит A, то $b > a$ для любого a из A. По теореме 7 тогда $b - 1 \geqslant a$ для любого a из A. Таким образом, число $b-1$ принадлежит B и $b - 1 < b$, что противоречит выбору числа b.

§ 15. Индуктивные определения. Сумма и произведение нескольких чисел

С индуктивными определениями мы уже имели дело при определении сложения и умножения. В обоих случаях при выборе определённого значения a дело шло о построении некоторой функции $f(b)$ числа b (значения которой — натуральные числа),

обладающей двумя свойствами: 1) известно значение функции для $b=1$ [в случае сложения $f(1)=a'$, в случае умножения $f(1)=a$]; 2) дано рекуррентное соотношение, однозначно определяющее значение функции для любого числа, отличного от 1, через её значение для предыдущего числа (в случае сложения $f(b)'=[f(b)]'$, в случае умножения $f(b')=f(b)+a$).

По поводу определения сложения мы уже указывали (§ 12), что такое определение ещё не доказывает (простым применением аксиомы индукции IV) существования и единственности функции $f(b)$ с указанными свойствами 1) и 2). Однако существование и единственность были доказаны разными путями как для сложения, так и для умножения. После определения порядка натуральных чисел можно доказать законность индуктивных определений и притом более общего типа, чем в случае сложения и умножения. А именно:

Определение 1. *Индуктивным определением* (или построением) *функции* $f(a)$ *на множестве натуральных чисел называется её определение по следующим двум свойствам*:

1) *задано значение функции* $f(1)=x_1$ *для числа* 1;

2) *значение функции* $f(a)$ *для натурального числа* $a>1$ *однозначно выражено через её значения* $f(b)$ *для натуральных чисел* $b<a$ *при помощи данной системы* S *рекуррентных соотношений.*

Отметим, что значения определяемой индуктивно функции $f(a)$ вовсе не обязательно должны быть натуральными числами. Они могут быть элементами некоторого кольца или вообще некоторого множества A, причём между его элементами определены отношения, при которых имеют смысл рекуррентные соотношения системы S.

Что индуктивное определение действительно определяет (и притом однозначно) функцию $f(a)$, показывает следующая:

Теорема 1. (Теорема о законности индуктивного определения.) *При данной системе* S *рекуррентных соотношений существует одна и только одна функция* $f(a)$, *заданная на множестве всех натуральных чисел и обладающая свойствами* 1) и 2), *указанными в определении* 1.

Докажем сначала такую лемму:

Лемма. *Пусть даны*: а) *натуральное число* n, б) *элемент* x_1 *некоторого множества* A, в) *при* $n>1$ *система* S *рекуррентных соотношений, которая для любого натурального числа* a (где $1<a\leqslant n$) *и любых элементов* x_b (где $b<a$) *множества* A *однозначно определяет элемент* x_a *того же множества* A [1]).

Тогда существует одна и только одна функция $f_n(a)$, *заданная на отрезке*[2]) $|1, n|$, *значения которой принадлежат множе-*

---

[1]) При этом для $a>n$ рекуррентные соотношения могут вообще не задаваться.

[2]) Отрезком натурального ряда (согласно определению 1 из § 4) называется множество $|1, n|$ натуральных чисел $a\leqslant n$.

ству A и которая обладает свойствами: 1) $f(1)=x_1$, 2_n) *при* $n>1$ *и* $1<a\leqslant n$ *значение* $f(a)$ *связано со значениями* $f(b)$ (где $b<a$) *рекуррентными соотношениями данной системы S.*

Доказательство леммы. Пусть M — множество тех n, для которых лемма верна.

А) Для $n=1$ условие в) и свойство 2_n) отпадают. Очевидно, $f(1)=x_1$ будет тогда единственной функцией, заданной на отрезке $|1, 1|$ и обладающей свойством 1); 1 принадлежит M.

Б) Если n принадлежит M, то для n лемма верна. Пусть условия а), б), в) леммы выполнены для числа $n+1$. Тогда эти условия выполняются также и для числа n [при той же системе S рекуррентных соотношений в пункте в) и том же x_1 в б)]. Стало быть, существует одна и только одна функция $f_n(a)$, заданная на отрезке $|1, n|$ и обладающая свойствами 1) и 2_n). Мы строим тогда функцию $f_{n+1}(a)$ следующим образом: для любого $a\leqslant n$ полагаем: $f_{n+1}(a)=f_n(a)$. Значение же $f_{n+1}(n+1)$ определяем по значениям $f_{n+1}(a)$ для $a<n+1$ из рекуррентных соотношений данной системы S, что возможно, так как условие в) выполнено для числа $n+1$. Тогда функция $f_{n+1}(a)$ задана на отрезке $|1, n+1|$ и обладает свойствами 1) и 2_{n+1}). Если $g(a)$ — любая функция, заданная на отрезке $|1, n+1|$ и обладающая свойствами 1) и 2_{n+1}), то эта функция $g(a)$ задана также на отрезке $|1, n|$ и обладает свойствами 1) и 2_n). В силу единственности такой функции (для n лемма верна) должно быть: $g(a)=f_n(a)$ для $a\leqslant n$. Но $g(a)$ обладает свойством 2_{n+1}). Следовательно, значение $g(n+1)$ однозначно определяется значениями $g(a)$ для $a\leqslant n+1$. Но для $a<n+1$, т. е. $a\leqslant n$,

$$g(a)=f_n(a)=f_{n+1}(a).$$

Поэтому также $g(n+1)=f_{n+1}(n+1)$. Итак, на всём отрезке $|1, n+1|$ функция $g(a)$ совпадает с $f_{n+1}(a)$, чем доказана единственность функции $f_{n+1}(a)$. Лемма доказана для числа $n+1$; $n+1$ принадлежит множеству M. По аксиоме IV M содержит все натуральные числа, т. е. лемма верна для любого натурального числа n.

Доказательство теоремы 1. Условия 1) в определении 1 и лемме совпадают. Из условия 2) определения 1 следует, что условие в) леммы выполнено при любом $n>1$. Согласно лемме для любого n существует одна и только одна функция $f_n(a)$, заданная на отрезке $|1, n|$ и обладающая свойствами 1) и 2_n). Если $m<n$, то функция $f_n(a)$ задана на отрезке $|1, m|$ как части отрезка $|1, n|$ и обладает свойствами 1) и 2_n), а стало быть и свойством 2_m). По единственности такой функции $f_n(a)=f_m(a)$ для $a\leqslant m$. Итак, все функции $f_n(a)$, определённые для числа a (т. е. при $n\geqslant a$), имеют для этого a одно и то же значение. Значение всех $f_n(a)$ при $n\geqslant a$ и примем за значение $f(a)$ искомой функции для числа a; $f(1)$ совпадает с $f_n(1)$, а так как $f_n(a)$ обладает свойством 1), то $f(a)$ обладает свойством 1). Если $a>1$ и $n\geqslant a$, то

$f(a)=f_n(a)$ и $f(a)$ также удовлетворяет рекуррентным соотношениям, т. е. функция $f(a)$ обладает свойством 2). Если $g(a)$ — любая функция, заданная на множестве натуральных чисел и обладающая свойствами 1) и 2), то она задана на любом отрезке $|1, n|$ и обладает там теми же свойствами. По единственности такой функции $g(a)=f_n(a)=f(a)$ при $n\geqslant a$. Таким образом, $g(a)=f(a)$ для любого a. Этим единственность функции $f(a)$, обладающей требуемыми свойствами, доказана.

На доказанной выше лемме основано введение понятий суммы и произведения нескольких натуральных чисел.

Определение 2. *Пусть даны натуральные числа*[1] $a_1, a_2, \ldots, a_n$, *где* n *— также натуральное число*[2]).

Суммой этих чисел называется число, которое обозначается через

$$a_1+a_2+\ldots+a_n=\sum_{i=1}^{n} a_i$$

и определяется условиями

$$\sum_{i=1}^{1} a_i=a_1, \tag{1}$$

$$\sum_{i=1}^{k+1} a_i=\sum_{i=1}^{k} a_i+a_{k+1} \tag{2}$$

для любого числа $k<n$.

Произведением этих чисел называется число, которое обозначается через

$$a_1\ a_2\ \ldots\ a_n=\prod_{i=1}^{n} a_i$$

и определяется условиями

$$\prod_{i=1}^{1} a_i=a_1, \tag{3}$$

$$\prod_{i=1}^{k+1} a_i=\left(\prod_{i=1}^{k} a_i\right) a_{k+1} \tag{4}$$

для любого числа $k<n$.

---

[1]) Это определение и все результаты данного параграфа дословно переносятся на любые кольца и вообще на любые множества, в которых определены операции сложения и умножения, подчинённые законам коммутативности и ассоциативности.

[2]) Строго говоря, на отрезке $|1, n|$ задана функция $f(b)=a_b$.

Условия (1) и (3) определяют значения данных функций числа k для $k=1$, а условия (2) и (4) играют роль рекуррентных соотношений в пункте в) леммы. По лемме существуют единственные функции $\sum_{i=1}^{k} a_i$ и $\prod_{i=1}^{k} a_i$, заданные на отрезке $|1, n|$ и обладающие соответственно свойствами (1), (2) и (3), (4). Поэтому определение 2 имеет точный смысл.

Замечание. До сих пор при построении арифметики натуральных чисел (начиная с § 11) мы нигде не пользовались теоремами первых двух глав; с другой стороны, в этих двух главах использовались лишь те понятия и факты из теории натуральных чисел (а именно, понятие отрезка натурального ряда, индуктивное доказательство и индуктивное определение), которые нами уже изложены. Поэтому, не делая порочного круга, мы можем в дальнейшем построении теории натуральных чисел опираться на факты из первых двух глав. В частности, верны основные свойства суммы и произведения [см. § 6, (1), (2)]:

$$\sum_{i=1}^{m} a_i + \sum_{i=1}^{n} a_{m+i} = \sum_{i=1}^{m+n} a_i; \quad \prod_{i=1}^{m} a_i \cdot \prod_{i=1}^{n} a_{m+i} = \prod_{i=1}^{m+n} a_i, \tag{5}$$

$$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i; \quad \prod_{i=1}^{n} (a_i b_i) = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i. \tag{6}$$

При совпадающих слагаемых или сомножителях сумма и произведение по определению дают кратное и соответственно степень натурального числа a. Для них верны обычные правила оперирования [см. § 6, (3)—(8)].

Итак, определением кратного и степени числа служат равенства

$$an = \sum_{i=1}^{n} a, \tag{7}$$

$$a^n = \prod_{i=1}^{n} a. \tag{8}$$

Но обозначение an в (7) имело уже раньше другой смысл. Так обозначалось произведение натуральных чисел a и n. Нужно доказать, что оба истолкования записи an совпадают. Когда это будет доказано, то, придав натуральному числу n количественное значение (как мощности множества), мы придём к школьному определению произведения an как суммы n слагаемых, равных a.

Аналогично можно придти к определению степени a^n как произведения n сомножителей, равных a. Итак, докажем теорему:

Теорема 2. *Для любых натуральных чисел a и n справедливо равенство*

$$an = \sum_{i=1}^{n} a, \tag{9}$$

где an означает произведение чисел a и n (в смысле определения из § 13). *В частности,*

$$n = 1 \cdot n = \sum_{i=1}^{n} 1,$$

т. е. любое натуральное число n равно сумме n единиц.

Доказательство. Для $n = 1$ согласно свойству 1) определения из § 13 и свойству (1) суммы имеем:

$$a \cdot 1 = a = \sum_{i=1}^{1} a.$$

Если $an = \sum_{i=1}^{n} a$, то по свойству 2) определения § 13 и свойству (2) суммы имеем:

$$a(n+1) = an + a = \sum_{i=1}^{n} a + a = \sum_{i=1}^{n+1} a.$$

По аксиоме IV теорема доказана.

§ 16. Вычитание и деление

Основные вопросы арифметики натуральных чисел, обоснование которых содержит трудности, связанные с аксиоматическим построением, нами уже изложены. Остановимся ещё на свойствах обратных операций.

Определение 1. *Вычитанием натуральных чисел называется действие, обратное сложению, т. е. соответствие, которое с числами a и b сопоставляет число $a - b$* (называемое *разностью a и b*) *такое, что*

$$(a - b) + b = a. \tag{1}$$

Отсюда в связи с определением и теоремой 3 из § 14 находим:

Теорема 1. *Разность $a - b$ существует тогда и только тогда, когда $a > b$. Если разность существует, то она единственна.*

Из (1), далее, имеем:

$$a - b < a. \tag{2}$$

Здесь и ниже предполагается (если нет других указаний), что все встречающиеся разности существуют.

Справедливо равенство

$$(a - b)\, c = ac - bc, \tag{3}$$

ибо

$$(a - b)\, c + bc = ac.$$

Далее из (1) и (3) следует

а) $$a - b = c - d \tag{4}$$

тогда и только тогда, когда $a + d = b + c$;

б) $$(a - b) + (c - d) = (a + c) - (b + d);$$

в) $$(a - b) - (c - d) = (a + d) - (b + c);$$

г) $$(a - b)(c - d) = (ac + bd) - (ad + bc).$$

Теорема 2. *Из* а) $b \gtreqless c$ *следует соответственно* б) $a - b \lesseqgtr a - c$, *и обратно.*

Доказательство. Докажем, что из б) следует а). Прибавив к обеим частям б) $b + c$, получим (§ 14, теорема 2): $a + c \lesseqgtr a + b$, откуда (§ 14, теорема 3) $c \lesseqgtr b$, $b \gtreqless c$. Таким образом из а) следует б).

Определение 2. *Делением называется действие, обратное умножению, т. е. соответственно сопоставляющее с числами a и b число* $\frac{a}{b} = a : b$ (называемое *частным a и b*) *такое, что*

$$\frac{a}{b} \cdot b = a. \tag{5}$$

Из $1 \leqslant b$ следует:

$$a \leqslant ab, \tag{6}$$

причём знак $=$ имеет место лишь для $b = 1$.

Отсюда и из (5)

$$\frac{a}{b} \leqslant a \tag{7}$$

со знаком $=$ лишь при $b = 1$.

Как и в случае вычитания, здесь и ниже предполагается, что все написанные частные существуют.

Теорема 3. *Из* а) $b \gtreqless c$ *следует соответственно* б) $\frac{a}{b} \lesseqgtr \frac{a}{c}$, *и обратно.*

Доказательство аналогично данному для теоремы 2.

Для частных справедливы правила сравнения и оперирования.

а) $$\frac{a}{b}=\frac{c}{d} \tag{8}$$

тогда и только тогда, когда $ad=bc$;

б) $$\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd};$$

в) $$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd};$$

г) $$\frac{a}{b}:\frac{c}{d}=\frac{ad}{bc}.$$

Доказываются они на основе теоремы 3 из § 14 дословно как соответствующие свойства частного в любом поле (§ 7, теорема 8). При этом в пунктах б), в) и г) из существования частных в левой части вытекает их существование в правой части.

Далее, из (6) и теоремы 3 § 14 находим:

Теорема 4. *Для того чтобы существовало частное* $\frac{a}{b}$, *необходимо* (но, как сейчас увидим, недостаточно), *чтобы было* $a\geqslant b$. *Если частное существует, то оно единственно.*

Что из $a\geqslant b$ ещё не следует существования частного $\frac{a}{b}$, показывают простые примеры. Так, определяя числа

$$2=1',\quad 3=2',\quad 4=3',$$

убеждаемся, что не существует a, для которого $2a=3$. Из (6) должно быть $a<3$, т. е. или $a=1$, или $a=2$, но $2\cdot 1=2$ и $2\cdot 2=4$.

Это обстоятельство обусловливает коренное различие свойств вычитания и деления и приводит к ряду свойств чисел, составляющих так называемую *теорию делимости*[1]).

§ 17. Замечания о системе аксиом натуральных чисел

Отправляясь от системы аксиом I—IV (§ 11), мы построили арифметику натуральных чисел. Вернёмся теперь снова к вопросам аксиоматического обоснования этой теории.

При оценке системы аксиом всякой аксиоматической теории приходится решать три основных вопроса (правда, неодинаковой трудности и значения) — это вопросы о непротиворечивости, полноте и независимости аксиом.

---

[1]) О свойствах делимости см. статью А. Я. Хинчина, помещённую в этой книге.

Непротиворечивость. Для приемлемости любой системы аксиом нужно, прежде всего, убедиться, что построенная на её основе теория не содержит противоречий, т. е. что с помощью этих аксиом нельзя доказать двух взаимно исключающих друг друга предложений. Как же можно доказать непротиворечивость аксиом данной системы в этом смысле? Разберём этот вопрос на примере плоской геометрии. При её аксиоматике точки и прямые, а также и основные отношения между ними («точка лежит на прямой», «одна точка прямой лежит между двумя другими» и т. д.) понимаются формально (абстрактно). Эти понятия связаны данной системой аксиом. С другой стороны, имеется другая аксиоматическая теория — поле действительных чисел. В аналитической геометрии устанавливается, что точкам плоскости соответствуют пары чисел (координаты точки), а прямым — уравнения (уравнения прямых). Отношениям между точками и прямыми соответствуют известные числовые отношения этих пар и уравнений, причём аксиомам геометрии соответствуют предложения (теоремы), которые можно доказать на основе аксиом и свойств чисел. Таким образом, одна аксиоматическая теория (геометрия плоскости) включается как часть в другую (теорию действительного числа). Если бы геометрия содержала противоречие в указанном выше смысле, то и для действительных чисел можно было бы найти противоречие (доказать на основе аксиом чисел два взаимно исключающих предложения). Если аксиоматика чисел непротиворечива, то то же верно и для аксиоматики геометрии. В этом смысле непротиворечивость аксиом геометрии доказана.

Представление одной аксиоматической теории при помощи понятий другой теории, разобранное нами на примере плоской геометрии и арифметики, применяется в математике весьма часто и не только для сведéния непротиворечивости одной теории к непротиворечивости другой. Поэтому мы дадим для него следующее определение:

Определение 1. *Любое множество, для элементов которого определены основные отношения и выполнены аксиомы данной аксиоматической теории, называется интерпретацией этой теории.*

Интерпретация данной аксиоматической теории не разрешает вопроса о её непротиворечивости, а лишь сводит его к вопросу о непротиворечивости той теории, в которой осуществлена данная интерпретация.

Непротиворечивость теории натуральных чисел доказана не формально-логическими средствами, а многовековой практикой человечества, показавшей отсутствие противоречий в этой теории и её соответствие с действительными соотношениями реального мира.

Полнота. Далее, возникает вопрос, насколько хорошо описывает система аксиом данную теорию? Можно ли с помощью данной системы аксиом доказать или опровергнуть любое предположение,

высказанное в терминах данной теории? Австрийский математик Гедель в 1931 г. доказал, что для ряда теорий, в том числе и для аксиоматической теории натуральных чисел, полнота в этом смысле отсутствует, т. е. существуют неразрешимые данными средствами предложения. Мы будем считать систему полной в ином смысле, именно, если она вполне определяет, т. е. до изоморфизма однозначно описывает, данное множество. Итак,

Определение 2. *Система аксиом называется полной, если две любые её интерпретации изоморфны* (§ 9, определение 1).

Примером неполной системы аксиом может служить система свойств I—VI, определяющая понятие кольца (§ 7). Ведь существуют неизоморфные кольца (хотя бы конечные и бесконечные). Более того, основной интерес теории колец и лежит в описании всех типов колец.

Докажем, что система аксиом I — IV натуральных чисел полна. Пусть N_1 и N_2 — две интерпретации этой системы. Числа в этих интерпретациях будем отличать индексами 1 и 2. Строим по индукции (§ 15, определение 1) функцию $f(x_1)$, заданную на всём множестве N_1, значение которой принадлежит N_2, и такую, что 1) $f(1_1)=1_2$, 2) $f(a_1')=[f(a_1)]'$.

По теореме 1 из § 15 такая функция существует и только одна. Покажем, что соответствие $f(a_1)=a_2$ является изоморфизмом N_1 и N_2. Если $a_1 \neq 1_1$, то $a_1=b_1'$ и

$$f(a_1)=f(b_1')=[f(b_1)]' \neq 1_2.$$

Итак, 1_2 имеет единственный прообраз в N_1, именно 1_1. Пусть a_2 имеет единственный прообраз a_1. Тогда

$$f(a_1')=[f(a_1)]'=a_2'.$$

Стало быть, a_2' имеет хотя бы один прообраз. Если b_1 — любой прообраз для a_2', то по 1) $b_1 \neq 1_1$, т. е. $b_1=c_1'$, и

$$a_2'=f(b_1)=f(c_1')=[f(c_1)]'.$$

По аксиоме III следует: $a_2=f(c_1)$, а так как a_1 — единственный прообраз a_2, то $c_1=a_1$ и по аксиоме II $b_1=c_1'=a_1'$. Следовательно, a_1' — единственный прообраз для a_2'. По аксиоме индукции IV любой элемент в N_2 имеет один и только один прообраз в N_1. Соответствие $f(a_1)=a_2$ взаимно однозначно. Из 2) следует, что отображение

$$f(a_1)=a_2, \quad N_1 \text{ на } N_2$$

сохраняет основное отношение «следует». Остаётся доказать это для обратного отображения $f^{-1}(a_2)=a_1$. Но из $f(a_1')=[f(a_1)]'=a_2'$ следует $f^{-1}(a_2')=a_1'$, т. е. и обратное отображение сохраняет отношение «следует».

Таким образом, система аксиом I — IV натуральных чисел полна. О значении этого факта уже говорилось в § 11. Только благодаря полноте системы аксиом I — IV мы можем с равным успехом пользоваться любой интерпретацией натуральных чисел (применяются ли римские или арабские цифры, десятичная или двоичная система счисления).

Независимость. Более простым и имеющим скорее практическое, чем принципиальное значение, является вопрос о независимости аксиом. При выборе той или иной системы аксиом для данной теории желательно достичь минимального числа положений, принимаемых за аксиомы. Если, например, одна из аксиом в действительности является теоремой, т. е. её можно доказать с помощью остальных аксиом, то нет надобности сохранять её в списке аксиом.

Определение 3. *Система аксиом называется независимой, если ни одна из аксиом не является следствием остальных.*

Доказательство независимости системы аксиом проводится так. Для каждой аксиомы строится интерпретация, где выполнены все остальные аксиомы, тогда как данная аксиома не выполняется. Если бы эта аксиома была следствием остальных, то такая интерпретация была бы, очевидно, невозможна.

Докажем независимость системы аксиом I — IV натурального ряда. Заметим, что доказательство независимости аксиомы I имеет ту особенность, что если аксиома I не выполнена, то аксиома IV становится бессодержательной, так как множеств M, содержащих единицу, вообще не существует, ибо не существует числа единицы. Поэтому для доказательства независимости аксиомы I от остальных аксиом мы несколько видоизменим формулировку аксиомы IV, заменив её следующей:

IV'. *Любое непустое множество M натуральных чисел, обладающее свойствами:* А) *если существует число* 1, *не следующее ни за каким другим числом, то оно принадлежит M;* Б) *если число a принадлежит M, то и следующее число a' принадлежит M — содержит все натуральные числа.*

Очевидно, что система аксиом I — III, IV эквивалентна системе I — III, IV', т. е. из первой системы следуют аксиомы второй, и обратно (достаточно убедиться, что из I — III, IV следует IV' и из I — III, IV' следует IV). Если одна из эквивалентных систем непротиворечива или полна, то то же верно и для другой. Итак, система аксиом I — III, IV' также непротиворечива и полна. Докажем её независимость.

1. Независимость аксиомы I. Пусть N — множество трёх элементов a, b, c с таким определением отношения «следует» [1])

$$a' = b, \quad b' = c, \quad c' = a.$$

[1]) Можно взять любое конечное множество с числом элементов $\geqslant 2$, расположенных в круговом порядке.

Так как всякий элемент следует за другим, то I не выполнено. II, III, IV′ выполнены. Если $M \neq 0$ и, например, $b \in M$, то по 2) также $b' = c \in M$ и $c' = a \in M$, $M = N$.

2. Независимость аксиомы II. Пусть N — множество двух элементов a и b, причём $a' = b$. Тогда a будет единицей. Аксиома II не выполнена, так как b не имеет следующего элемента.

Прочие аксиомы выполнены.

3. Независимость аксиомы III. Пусть N — множество четырёх элементов a, b, c, d, причём

$$a' = b, \quad b' = c, \quad c' = d, \quad d' = b.$$

Аксиома III не выполнена, так как b следует за a и d, из $a' = d'$ не следует $a = d$. Остальные аксиомы выполнены, причём a играет роль единицы.

4. Независимость аксиомы IV′ (или также IV). Пусть N — множество всех натуральных чисел 1, 2, 3, ..., n, ... и всех чисел вида $n + \frac{1}{2}$ с любым целым n, причём для натуральных чисел отношение «следует» имеет прежний смысл и

$$\left(n + \frac{1}{2}\right)' = n + \frac{3}{2}.$$

Аксиома IV′ не выполнена. В самом деле, роль единицы играет само число 1 (только оно не следует ни за каким другим). Множество M всех натуральных чисел обладает сзойствами А′) и Б) [или А) и Б) при аксиоме IV], но не содержит всех элементов множества N.

Таким образом, система аксиом I—III, IV натуральных чисел независима.

ГЛАВА IV

КОЛЬЦО ЦЕЛЫХ ЧИСЕЛ

§ 18. Принцип расширения в арифметике и алгебре

Понятие числа прошло длинный путь исторического развития. Натуральные числа как средство счёта известны человеку на самых ранних ступенях развития. Древнегреческие математики пользовались как натуральными, так и дробными положительными числами, но не знали отрицательных чисел. Употребление положительных и отрицательных чисел (толкуемых как «имущество» и «долг») впервые появилось у индусов (Арьябхатта, р. 476 г.; Брамагупта, 588?—660 гг.; Бхаскара р. 1114 г.).

Современное обозначение положительных и отрицательных чисел знаками $+$ и $-$ введено в конце XIV в. немецким математиком Видманном. Однако ещё в XVI в. многие математики не признавали отрицательных чисел. Так, французский математик Виет (1540—1603) при выводе соотношений между корнями и коэффициентами уравнения ограничивался случаем положительных корней. Полное признание отрицательные числа получили лишь в XVII в.

Таким образом, дробные числа появились в математике намного раньше отрицательных. Возникновение дробных чисел связано с задачами измерения.

Отступая от исторического пути развития по соображениям большей логической простоты, мы введём сначала все целые числа, а затем уже числа дробные.

Натуральные числа служат фундаментом, на котором чисто конструктивным путём можно построить все другие числовые множества. Мы последовательно определим целые, рациональные, действительные и комплексные числа. Каждое из перечисленных числовых множеств содержит предыдущее. При этом мы стремимся построить расширение, обладающее известными свойствами по отношению к расширяемому множеству. Если множество A расширяется до множества B, то эти свойства сводятся к следующему:

1) A есть подмножество B.

2) Интересующие нас операции или вообще отношения элементов множества A определены также и для элементов множества B,

причём их смысл для элементов A, рассматриваемых уже как элементы B, должен совпадать с тем, какой они имели в A до расширения.

3) В B должна быть выполнима операция, которая в A была невыполнима или не всегда выполнима.

Это требование служит основной целью, для достижения которой строится расширение. Разберём его на примерах. Для натуральных чисел не всегда выполнимо вычитание. В области целых чисел оно всегда выполнимо. Для целых чисел не всегда выполнимо деление. Для рациональных чисел оно выполнимо всегда (кроме деления на 0, что вообще невозможно). Для рациональных чисел не всегда выполнима операция перехода к пределу. Для действительных чисел она всегда выполнима. Для действительных чисел не всегда выполнима операция извлечения корня. Для комплексных чисел она уже всегда выполнима.

Наконец, требования логической завершённости диктуют ещё одно условие:

4) Расширение B должно быть минимальным из всех расширений данного A, обладающих свойствами 1) — 3), и определяться данным A однозначно с точностью до изоморфизма.

Так, мы расширяем множество натуральных чисел до целых, а не сразу до действительных или комплексных.

Целые числа подразделяются на положительные (или натуральные), отрицательные и число 0. Идея отрицательного числа (всё равно целого, рационального или вообще действительного) связана с измерением величины, имеющей два противоположных смысла. Таковы, например, длины отрезков, откладываемых на прямой направо или налево от данной точки, показания термометра вверх и вниз от точки 0 и т. д. Тогда уславливаются величины одного смысла или направления измерять при помощи обычных чисел, называемых теперь положительными, а величины другого, противоположного смысла теми же числами, но снабжёнными особым знаком «—» для отличия их от чисел, служащих для выражения величин первого смысла. Затем формально вводится число 0, отделяющее положительные числа от отрицательных. Не останавливаясь на деталях такого введения «относительных» чисел, заметим, что это построение наиболее естественно, так как связано с их возникновением и может быть проведено строго формально. Так, для построения целых «относительных» чисел можно формально натуральным числам $a, b, \ldots$ поставить во взаимно однозначное соответствие новые объекты $\bar{a}, \bar{b}, \ldots$ и ввести ещё один объект 0. Затем определить сумму, произведение и отношение «больше» по известным школьным правилам и доказать (путём проверки всех случаев) справедливость всех законов действий и порядка.

Руководствуясь, однако, единством идеи, мы примем другое построение. Дело в том, что, желая при расширении сделать вы-

полнимой в B некоторую операцию, не всегда выполнимую в A, мы можем ввести формально в B те же правила оперирования, которые для данной операции имели место в A в тех случаях, когда она была там выполнима. Это формальное перенесение старых правил на новое множество и приводит к конструкции желаемого расширения. Так, разность $a-b$ для натуральных чисел вполне определяется парой чисел a, b. Такую пару мы и примем за исходный пункт определения целого числа, сохраняя правила оперирования, справедливые для разностей $a-b$ натуральных чисел. Та же идея лежит в основе конструкции рациональных и комплексных чисел, а также алгебраических дробей. Эта конструктивная идея носит название *теории пар*. Заметим, что во всех указанных случаях конструкция приводит не сразу к желаемому расширению B для области A, а лишь к области B', изоморфной области B и содержащей подмножество A', изоморфное A. Искомое расширение B получится из B' заменой в нём A' на A. Но до проведения такого построения целых чисел необходимо сделать некоторые замечания, связанные с основными свойствами равенства.

§ 19. Эквивалентность и разбиение на классы

Равенство $a=b$ элементов некоторого множества мы всегда понимаем как отношение между элементами, заключающееся в их совпадении или тождестве [1]).

Отсюда по чисто логическим основаниям вытекают следующие основные свойства равенства: а) $a=a$ (рефлексивность или закон тождества); б) если $a=b$, то $b=a$ (симметрия); в) если $a=b$ и $b=c$, то $a=c$ (транзитивность).

Но теми же свойствами обладают, как мы видели, и другие отношения, именно: равномощность $A\sim B$ (§ 3), подобие $A\approx B$ (§ 5), изоморфизм $A\cong B$ (§ 9).

Для всех таких отношений мы докажем следующую общую теорему.

Теорема. *Если для элементов множества M определено отношение эквивалентности $a\sim b$ (словами: a эквивалентно b), обладающее следующими свойствами*: 1) $a\sim a$, 2) *если* $a\sim b$, *то* $b\sim a$, 3) *если* $a\sim b$ *и* $b\sim c$, *то* $a\sim c$, *то этим однозначно определено разбиение множества M на попарно непересекающиеся подмножества, обладающие тем свойством, что любые элементы одного и того же подмножества эквивалентны и любые элементы различных подмножеств неэквивалентны* (*разбиение на классы эквивалентных элементов*).

---

[1]) Многие авторы считают равенство некоторым понятием, подлежащим определению или аксиоматическому описанию.

Обратно, *для любого разбиения множества M на непересекающиеся подмножества можно так определить отношения эквивалентности, что данное разбиение M будет разбиением на классы эквивалентных элементов.*

Доказательство. а) Пусть дано отношение эквивалентности. Для каждого $a \in M$ обозначим через M_a множество всех элементов x, для которых $x \sim a$. Из 1) следует, что $a \in M_a$, т. е. любой элемент множества M принадлежит некоторому из этих подмножеств. Пусть $b \in M_a$ и $c \in M_a$. Тогда $b \sim a$, $c \sim a$; по 2) также $a \sim c$ и по 3) $b \sim c$. Следовательно, два элемента из M_a эквивалентны. Если $a \sim b$, то $M_a = M_b$. В самом деле, если $c \in M_a$, то $c \sim a$, $a \sim b$ и по 3) $c \sim b$, т. е. $c \in M_b$. Если же $c \in M_b$, то $c \sim b$ и $a \sim b$; по 2) $b \sim a$ и по 3) $c \sim a$, т. е. $c \in M_a$. Отсюда также имеем: если $b \in M_a$, то $M_b = M_a$, т. е. все элементы множества M_a равноправны при определении этого множества. Если множества M_a и M_b имеют общий элемент c, то $M_c = M_a$, $M_c = M_b$, откуда $M_a = M_b$. Таким образом, два различных множества не могут иметь общих или эквивалентных элементов. Элементы различных множеств неэквивалентны.

б) Пусть дано разбиение множества M на непересекающиеся множества. Определим отношение эквивалентности элементов M так: $a \sim b$, если a и b принадлежат одному и тому же множеству данного разбиения. Очевидно, что тогда разбиение на классы эквивалентных элементов и будет данным разбиением.

Доказанная теорема найдёт в будущем неоднократное применение, позволяя опускать приведённое рассуждение в каждом конкретном случае.

§ 20. Определение кольца целых чисел

Для натуральных чисел не всегда выполнима операция, обратная сложению, т. е. вычитание (§ 16, теорема 1). Поставим задачу расширить множество N натуральных чисел до такого множества C, где были бы заданы операции сложения и умножения, обладающие теми же свойствами, какими они обладают для натуральных чисел, причём вычитание было бы всегда возможно. Это значит, что C должно быть кольцом (§ 7, определение 1). Будем искать минимальное из таких расширений в смысле следующего определения:

Определение 1. *Кольцом целых чисел называется минимальное кольцо C, содержащее множество N всех натуральных чисел, т. е. множество, обладающее свойствами*: 1) *C содержит N;* 2) *C есть кольцо*; 3) *сложение и умножение натуральных чисел совпадают с одноимёнными операциями над этими числами в кольце C*; 4) *кольцо C не содержит отличного от него подкольца, содержащего множество N. Элементы кольца C называются целыми числами.*

Из этого определения ещё неясно, существует ли такое кольцо C и будет ли оно единственным. Отложив пока вопрос о существовании кольца целых чисел, покажем, что если оно существует, то будет единственным с точностью до изоморфизма.

Теорема 1. *Кольцо C, содержащее множество N натуральных чисел*[1]*, тогда и только тогда будет кольцом целых чисел* (т. е. минимальным)*, когда каждый его элемент равен разности натуральных чисел.*

Доказательство. А) Если кольцо C содержит N и каждый элемент C равен разности натуральных чисел, то C минимально, так как любое подкольцо, содержащее N, содержит и все разности натуральных чисел (§ 7, теорема 4) и, следовательно, совпадает с C.

Б) Пусть, обратно, кольцо C минимально. Во всяком кольце разность элементов обладает следующими свойствами (§ 7, теорема 3):

$$\left.\begin{array}{ll} \text{а)} & a-b=c-d \\ \multicolumn{2}{l}{\text{тогда и только тогда, когда } a+d=b+c;} \\ \text{б)} & (a-b)+(c-d)=(a+c)-(b+d); \\ \text{в)} & (a-b)-(c-d)=(a+d)-(b+c); \\ \text{г)} & (a-b)(c-d)=(ac+bd)-(ad+bc). \end{array}\right\} \quad (1)$$

Пусть R — множество всех элементов C, каждый из которых равен разности натуральных чисел. Из (1) следует, что сумма, разность и произведение двух элементов множества R снова принадлежат R, следовательно, R — подкольцо C. Любое натуральное число равно, конечно, разности натуральных чисел, например $a=(a+b)-b$, где b — также натуральное число. Так как операции в N и C совпадают, то R содержит N, и следовательно, $R=C$ в силу минимальности C. Это значит, что любое целое число равно разности натуральных чисел.

Теорема 2. *Все минимальные кольца, содержащие натуральные числа, изоморфны, т. е. кольцо целых чисел единственно с точностью до изоморфизма.*

Пусть C_1 и C_2 — два таких кольца. По предыдущей теореме любой элемент в C_1 и C_2 равен разности натуральных чисел. Строим такое отображение f кольца C_1 на C_2: если $c_1 \in C_1$ и $c_1=a-b$ в C_1, где a и b — натуральные числа, то в C_2 будет: $a-b=c_2$[2]).

---

[1]) Здесь и ниже, говоря, что кольцо содержит натуральные числа или что одно кольцо содержит другое, мы всегда будем подразумевать, что операции в подмножестве совпадают с соответствующими операциями в надмножестве.

[2]) Из $c_1=a-b$ и $c_2=a-b$ не следует $c_1=c_2$, так как вычитание в C_1 и C_2 может иметь разный смысл. Конечно, $c_1=c_2$ при $a>b$, так как тогда $a-b$ существует в N и по совпадению операций c_1 и c_2 равны одному и тому же натуральному числу $a-b$.

Тогда положим $f(c_1)=c_2$; c_2 не зависит от выбора чисел a и b. В самом деле, если также $c_1=c-d$, то $a-b=c-d$ и по (1) $a+d=b+c$, следовательно, и в C_2 также $a-b=c-d$. Если $c_1\neq d_1$, то по (1) также $f(c_1)\neq f(d_1)$. Любой элемент $c_1\in C_1$ равен разности натуральных чисел и то же верно для C_2. Итак, f — взаимно однозначное отображение C_1 на C_2. Из б), г) следует, что

$$f(c_1+d_1)=f(c_1)+f(d_1) \quad \text{и} \quad f(c_1d_1)=f(c_1)f(d_1)$$

для любых c_1, d_1 из C_1, т. е. f — изоморфизм колец C_1 и C_2 (§ 9, определение 2). Рассмотрим, например, первое из этих равенств. Если в C_1 имеем: $c_1=a-b$, $d_1=c-d$, то в C_2 будет:

$$f(c_1)=a-b, \quad f(d_1)=c-d,$$

откуда

$$f(c_1)+f(d_1)=(a-b)+(c-d)=(a+c)-(b+d),$$

но в C_1

$$c_1+d_1=(a+c)-(b+d),$$

т. е. элементы $c_1+d_1\in C_1$ и $f(c_1)+f(d_1)\in C_2$ равны разности одних и тех же натуральных чисел $a+c$ и $b+d$.

Это следует из определения f и, таким образом,

$$f(c_1+d_1)=f(c_1)+f(d_1).$$

Аналогично доказывается и второе соотношение. Теорема доказана.

Замечание. Изоморфное отображение f обладает ещё тем свойством, что на множестве N оно является тождественным, т. е. при этом отображении C_1 на C_2 каждое натуральное число отображается само на себя. В самом деле, при $c_1=a-b$ в C_1 и $c_2=a-b$ в C_2 элементы c_1 и c_2 тогда и только тогда будут сами натуральными числами, когда $a>b$. При этом $c_2=f(c_1)=a-b=c_1$.

Теорема 3. *Любое кольцо R, содержащее множество натуральных чисел N, содержит и кольцо целых чисел.*

Доказательство. Пересечение всех подколец кольца R, содержащих N, есть опять подкольцо (§ 8, теорема 6), содержащее N, и при этом минимальное, так как оно входит в любое подкольцо, содержащее N. Согласно определению 1 это подкольцо будет кольцом целых чисел.

Мы ещё пока не доказали существования кольца целых чисел, так как не построили ни одного примера (ни одной интерпретации) этого понятия. Перейдём теперь к построению такого примера.

Конструкция одного из изоморфных колец целых чисел подсказывается теоремой 1. Если C — кольцо целых чисел, то элементами C будут разности натуральных чисел. Можно было бы за элементы искомого кольца принять самые символы этих разностей $a-b$, но, во-первых, два таких символа, различных между собой, должны были бы считаться при некоторых условиях согласно (1)

равными ($a-b=c-d$, если $a+d=b+c$), что не согласуется с нашим условием понимать под равенством элементов любого множества их совпадение, а, во-вторых, мы желаем сохранить обозначение $a-b$ за операцией вычитания в искомом кольце.

За исходный элемент конструкции примем пару a, b натуральных чисел, взятых в данном порядке. Пусть M — множество всех таких пар. Определим отношение эквивалентности пар так, чтобы разности чисел эквивалентных и только эквивалентных пар были равны одному и тому же элементу искомого кольца. Согласно (1) определяем эквивалентность так:

$$(a, b)\sim(c, d), \tag{2}$$

тогда и только тогда, когда $a+d=b+c$.

Далее, определяем сложение и умножение пар так, чтобы в искомом кольце этим операциям соответствовали сложение и умножение разностей чисел, образующих данные пары. Согласно б), г) мы поэтому определяем:

$$(a, b)+(c, d)=(a+c, b+d), \tag{3}$$

$$(a, b)(c, d)=(ac+bd, ad+bc). \tag{4}$$

Теорема 4. *Сложение и умножение пар коммутативны, ассоциативны и связаны законом дистрибутивности.*

Доказательство. Эти свойства вытекают из соответствующих свойств натуральных чисел и доказываются непосредственной проверкой. Докажем, например, ассоциативность умножения:

$$[(a, b)(c, d)](e, f)=(ac+bd, ad+bc)(e, f)=$$
$$=(ace+bde+adf+bcf, acf+bdf+ade+bce);$$
$$(a, b)[(c, d)(e, f)]=(a, b)(ce+df, cf+de)=$$
$$=(ace+adf+bcf+bde, acf+ade+bce+bdf).$$

Получившиеся в итоге пары равны, т. е.

$$[(a, b)(c, d)](e, f)=(a, b)[(c, d)(e, f)].$$

Отношения эквивалентности пар (2) обладают свойствами 1)—3) из теоремы § 19. Действительно,

1) $(a, b)\sim(a, b)$, ибо $a+b=b+a$.

2) Если $(a, b)\sim(c, d)$, то $(c, d)\sim(a, b)$, ибо если $a+d=b+c$, то $c+b=d+a$

3) Если $(a, b)\sim(c, d)$ и $(c, d)\sim(e, f)$, то $(a, b)\sim(e, f)$, ибо, складывая равенства $a+d=b+c$, $c+f=d+e$, получим: $a+d+c+f=b+c+d+e$, откуда $a+f=b+e$ (§ 14, теорема 3).

Итак, отношение эквивалентности определяет разбиение множества M всех пар на классы эквивалентных пар. Будем обозначать эти классы малыми греческими буквами α, β, γ, δ, ...

Определение 2. *Пусть C_0 есть множество всех классов эквивалентных пар множества M. Суммой (произведением) двух классов α и β назовём тот класс $\alpha+\beta$ (соответственно $\alpha\beta$), который содержит сумму (произведение) пары класса α и пары класса β.*

Как всегда при определении операций над классами через операции над представителями этих классов, надо показать, что результат операции не зависит от выбора представителей. Это следует, очевидно, из такой теоремы:

Теорема 5. *Если*

$$(a_1,\ b_1)\sim(a_2,\ b_2) \quad \text{и} \quad (c_1,\ d_1)\sim(c_2,d_2),$$

то

$$(a_1,\ b_1)+(c_1,\ d_1)\sim(a_2,\ b_2)+(c_2,\ d_2),$$
$$(a_1,\ b_1)(c_1,\ d_1)\sim(a_2,\ b_2)(c_2,\ d_2).$$

Доказательство. Докажем, что из $(a_1,\ b_1)\sim(a_2,\ b_2)$ для любой пары (c, d) следует: $(a_1,\ b_1)+(c,\ d)\sim(a_2,\ b_2)+(c,\ d)$ и $(a_1,\ b_1)(c,\ d)\sim(a_2,\ b_2)(c,\ d)$.

В самом деле, $a_1+b_2=a_2+b_1$, откуда

$$(a_1+c)+(b_2+d)=(a_2+c)+(b_1+d),$$

т. е.

$$(a_1,\ b_1)+(c,\ d)\sim(a_2,\ b_2)+(c,\ d).$$

Умножая обе части равенства $a_1+b_2=b_1+a_2$ на c и — после перестановки левой и правой его частей — на d, получим:

$$a_1c+b_2c=b_1c+a_2c, \quad b_1d+a_2d=a_1d+b_2d.$$

Складывая, находим:

$$(a_1c+b_1d)+(a_2d+b_2c)=(b_1c+a_2d)+(a_2c+b_2d),$$

откуда

$$(a_1,\ b_1)(c,\ d)\sim(a_2,\ b_2)(c,\ d).$$

Применяя дважды только что доказанные законы коммутативности сложения и умножения пар, найдём:

$$(a_1,\ b_1)+(c_1,\ d_1)\sim(a_2,\ b_2)+(c_1,\ d_1)\sim(a_2,\ b_2)+(c_2,\ d_2),$$
$$(a_1,\ b_1)(c_1,\ d_1)\sim(a_2,\ b_2)(c_1,\ d_1)\sim(a_2,\ b_2)(c_2,\ d_2).$$

Итак, определение 2 действительно вводит во множестве C_0 классов эквивалентных пар однозначно определённые операции сложения и умножения.

Теорема 6. *Множество C_0 с операциями, указанными в определении 2, есть кольцо.*

Доказательство. Нужно проверить выполнение в C_0 аксиом I—VI (§ 7, определение 1). Так как операции в C_0 определены для классов через представителей этих классов, то выполнение аксиом I, II, IV, V и VI следует из теоремы 4.

Займёмся аксиомой III. Пусть даны две пары (a, b) и (c, d). Если бы существовала пара (x, y), для которой $(a, b)+(x, y)=(c, d)$, то $a+x=c$, $b+y=d$, т. е. $a<c$, $b<d$. Поэтому, если имеет место хотя бы одно из условий $a\geqslant c$, $b\geqslant d$, то такой пары (x, y) не существует. Таким образом, вычитание пар не всегда возможно, т. е. сами пары кольца не образуют. Тем не менее C_0 будет кольцом. Пусть α и β два класса из C_0, причём α содержит пару (a, b) и β — пару (c, d). Надо найти класс γ такой, что $\alpha+\gamma=\beta$. Если (x, y) — пара искомого класса γ, то вовсе не нужно, чтобы выполнялось равенство $(a, b)+(x, y)=(c, d)$, а достаточно лишь эквивалентности $(a, b)+(x, y)\sim(c, d)$. Предположим сначала, что пара (x, y) с этим свойством существует. Тогда $(a+x, b+y)\sim(c, d)$, откуда $a+x+d=b+y+c$ или $(a+d)+x=(b+c)+y$. По определению эквивалентности (2) $(x, y)\sim(b+c, a+d)$.

По теореме 5 достаточно проверить, что хотя бы одна пара (x, y) с этим условием обладает требуемым свойством, т. е. удовлетворяет соотношению $(a, b)+(x, y)\sim(c, d)$. Но сама пара $(b+c, a+d)$ обладает нужным свойством. Действительно,

$$(a, b)+(b+c, a+d)=(a+b+c, b+a+d)\sim(c, d).$$

Этим доказано существование класса γ, для которого $\alpha+\gamma=\beta$. Теорема доказана.

Из существования класса γ со свойством $\alpha+\gamma=\beta$ вытекает его единственность (§ 6, теорема 1).

Выясним, какой смысл имеют в кольце C_0 нуль и противоположный элемент.

Нуль по его определению — такой класс 0, что $\alpha+0=\alpha$ для любого класса α. Если α содержит пару (a, b) и 0 — пару (x, y), то должно быть $(a, b)+(x, y)\sim(a, b)$. Отсюда, как в доказательстве последней теоремы, с заменой (c, d) на (a, b) получим:

$$(x, y)\sim(b+a, a+b)=(a+b, a+b)=(k, k).$$

По (2) любая такая пара действительно удовлетворяет условию

$$(a, b)+(k, k)\sim(a, b).$$

Итак, нулём кольца C_0 является класс 0, содержащий все пары с равными элементами.

Противоположный элемент для класса α — это такой класс $-\alpha$, для которого $\alpha+(-\alpha)=0$. Если α содержит (a, b) и $-\alpha$ содержит (x, y), то $(a, b)+(x, y)=(k, k)$. Здесь можно писать не $\sim$, а $=$, так как по (2) пара, эквивалентная паре (k, k), сама имеет

равные элементы; следовательно, $a+x=b+y$, откуда $(x, y)=$ $=(b, a)$. Но сама пара (b, a) обладает нужным свойством, ибо

$$(a, b)+(b, a)=(a+b, b+a)$$

принадлежит классу 0. Назовём пару (b, a) *противоположной* (a, b). При замене пары (a, b) эквивалентной противоположная пара также заменяется на эквивалентную; любая пара класса $-\alpha$ противоположна некоторой паре класса α.

Итак, класс $-\alpha$, противоположный классу α, состоит из пар, противоположных парам класса α.

Построенное нами кольцо C_0 является изоморфным кольцу целых чисел. Если строить целые числа лишь с точностью до произвольного изоморфизма, то само C_0 можно считать кольцом целых чисел. Однако, при расширении данной системы чисел до новой мы будем считать эту данную систему определённой вполне однозначно, т. е. из всех её интерпретаций выбираем какую-нибудь одну. При этом условии кольцо C_0 не удовлетворяет определению 1, так как C_0 не содержит натуральных чисел, ибо его элементы — классы эквивалентных пар натуральных чисел.

Так как натуральные числа сами ещё не являются элементами кольца C_0, то для получения из C_0 кольца целых чисел (определение 1) надо включить в C_0 множество натуральных чисел N.

Сначала найдём в кольце C_0 множество, изоморфное множеству натуральных чисел. Любой класс α кольца C_0, отличный от нуля, состоит из пар (a, b), где $a\neq b$. Назовём класс α *классом первого рода*, если $a>b$, и *второго рода*, если $a<b$. Это определение не зависит от выбора пары (a, b) в классе α, так как если $(a, b)\sim$ $\sim(c, d)$, то $a+d=b+c$. Поэтому из $a>b$ следует (§ 16, теорема 2) $d<c$, $c>d$, из $a<b$ следует также $c<d$. Пусть N_1 и N_2 — соответственно множества классов первого и второго рода. Покажем, что множество N_1 классов первого рода изоморфно множеству N натуральных чисел относительно операций сложения и умножения. Построим взаимно однозначное отображение f множества N_1 на N. Если класс α из N_1 содержит пару (a, b), то $a>b$ и, следовательно, существует натуральное число k такое, что $a=$ $=b+k$ (§ 14). Мы положим $f(\alpha)=k$. Число k не зависит от выбора пары класса α, так как из $(a, b)\sim(c, d)$, т. е. $a+d=b+c$ при $a=b+k$, следует $b+k+d=b+c$, откуда также $c=d+k$. Разным классам соответствуют разные числа, так как если α содержит (a, b) и β содержит (c, d), причём $f(\alpha)=f(\beta)=k$, то $a=b+k$, $c=d+k$ и, складывая крест-накрест, найдём:

$$a+d+k=b+k+c,\quad a+d=b+c,\quad (a, b)\sim(c, d),\quad \alpha=\beta.$$

Любое число k является образом некоторого класса α, именно содержащего пару $(a+k, a)$. Этим доказано, что отображение f взаимно однозначно (§ 3, определение 3).

Покажем, что N_1 и N изоморфны относительно определённых в них сложения и умножения, т. е. покажем справедливость равенств

$$f(\alpha)+f(\beta)=f(\alpha+\beta),\quad f(\alpha)f(\beta)=f(\alpha\beta). \tag{5}$$

В самом деле, если α содержит пару $(a+k,\ a)$ и β — пару $(b+l,\ b)$, то $\alpha+\beta$ содержит пару $(a+b+k+l,\ a+b)$, и, следовательно,

$$f(\alpha+\beta)=k+l=f(\alpha)+f(\beta).$$

Далее, $\alpha\beta$ содержит

$$(a+k,\ a)\cdot(b+l,\ b)=$$
$$=(ab+kb+al+kl+ab,\ ab+kb+ab+al)=(c+kl,\ c),$$

где $c=2ab+al+bk$. Следовательно,

$$f(\alpha\beta)=kl=f(\alpha)f(\beta).$$

Построим теперь искомое кольцо целых чисел C. Рассуждения будут аналогичными с доказательством соответствующей теоремы о кольцах (§ 9, теорема 2). Пусть C — множество, полученное из кольца C_0 путём замены всех классов первого рода натуральными числами, соответствующими этим классам при отображении f. Если дополним определение отображения f, полагая $f(\alpha)=\alpha$ для любого класса α второго рода и для $\alpha=0$, то получим взаимно однозначное отображение C_0 на C. Определим сложение и умножение во множестве C следующими равенствами:

$$f(\alpha)+f(\beta)=f(\alpha+\beta),\quad f(\alpha)f(\beta)=f(\alpha\beta). \tag{5'}$$

Здесь α и β — любые классы кольца C_0. Так как f — взаимно однозначное отображение C_0 на C, то $f(\alpha)$ и $f(\beta)$ — любые элементы C. Далее, сумма $\alpha+\beta$ и произведение $\alpha\beta$ определены в C_0 однозначно, и равенства (5') действительно определяют операции сложения и умножения для любых элементов множества C.

Итак, C — множество с двумя операциями. Одновременно равенства (5') показывают, что множество C с так определёнными операциями изоморфно кольцу C_0 и само является кольцом (§ 9, теорема 1).

Теорема 7. *Кольцо C, построенное выше, есть кольцо целых чисел.*

Доказательство. Надо доказать, что C обладает свойствами 1) — 4), указанными в определении 1 в начале этого параграфа. Мы уже знаем, что 1) C содержит множество N натуральных чисел и 2) C есть кольцо.

Если $k=f(\alpha)$ и $l=f(\beta)$ — натуральные числа, то α и β — классы первого рода. Тогда равенства (5'), определяющие в кольце C сумму $k+l$ и произведение kl, совпадают соответственно с равенствами (5), где сложение и умножение в левых частях являются операциями, определёнными для натуральных чисел в §§ 12, 13. Итак:

3) Сложение и умножение натуральных чисел совпадают с одноимёнными операциями для этих чисел в кольце C.

Покажем, что любой элемент кольца C равен разности натуральных чисел. Любой элемент C имеет вид $f(\alpha)$, где α — класс кольца C_0 и f — построенное выше отображение C_0 на C. Пусть α содержит пару (k, l), причём $k=f(\beta)$, $l=f(\gamma)$. По определению отображения f класс β состоит из пар вида $(b+k, b)$ и γ — из пар вида $(c+l, c)$, следовательно, класс $\alpha+\gamma$ содержит пару $(k, l)+(c+l, c)=(k+c+l, l+c)$, принадлежащую β, откуда $\alpha+\gamma=\beta$. Итак, по определению сложения в кольце C, т. е. по (5′) [1]:

$$f(\alpha)+f(\gamma)=f(\beta), \quad \text{т. е.} \quad f(\alpha)=f(\beta)-f(\gamma)=k-l\ ^{2}).$$

Любое подкольцо C, содержащее натуральные числа, должно содержать все их разности и совпадает с C. Следовательно,

4) Кольцо C не содержит никакого подкольца, содержащего N и отличного от самого C.

Итак, одно из изоморфных между собой колец целых чисел нами построено. Его элементами (т. е. целыми числами) являются: во-первых, все натуральные числа, во-вторых, число 0, т. е. класс всех пар натуральных чисел с равными элементами, в-третьих, все классы второго рода, т. е. классы эквивалентных пар (a, b) натуральных чисел с условием $a<b$. Этим решён вопрос о существовании кольца целых чисел.

Пока читателю трудно узнать в построенном выше кольце C так хорошо известное ему кольцо целых чисел. В следующем параграфе мы рассмотрим простейшие свойства этого кольца и увидим, что оно ничем не отличается от всем известной совокупности целых чисел.

§ 21. Свойства целых чисел

Замечание 1. Для целых чисел как для элементов кольца верны все правила оперирования, доказанные в § 7. Так, произведение нуля на любое число равно нулю [§ 7, (2)], верны обычные правила знаков при умножении [§ 7, (3)] и т. д.

Теорема 1. *Натуральчыми числами* 1, 2, 3, ..., *числом* 0 *и числами* —1, —2, —3, ..., *противоположными натуральным, исчерпывается всё кольцо целых чисел* C, *т. е. для любого элемента* $a\in C$ *имеет место один и только один из трёх случаев*: a — *натуральное число,* $a=0$, $-a$ — *натуральное число.*

Доказательство. Пусть $a=f(\alpha)$, где α — класс кольца C_0 [3]). Выше было доказано, что α либо первого рода, либо 0, либо

[1]) Заметим, что нельзя применять (5), так как класс α не обязательно первого рода.

[2]) Для класса второго рода и 0, содержащихся в C, доказанное означает, что класс, содержащий пару (k, l), равен разности $k-l$.

[3]) Мы применяем, таким образом, для чисел, отличных от натуральных, обозначения как греческими, так и латинскими буквами, считая $a=\alpha$.

второго рода. Эти случаи несовместимы, так как если (k, l) — пара класса α, то соотношения $k > l$, $k = l$, $k < l$ несовместимы (§ 14, теорема 1). Если α — второго рода, то $k < l$. Тогда противоположный класс $-\alpha$ содержит пару (l, k), где $l > k$, т. е. он первого рода. При изоморфизме f свойство элементов быть противоположными друг другу сохраняется, т. е.

$$f(-\alpha) = -f(\alpha) = -a.$$

Если α первого рода, то $a = f(\alpha)$ — натуральное число по определению f; если $\alpha = 0$, то $a = \alpha = 0$; если a — второго рода, то $-\alpha$ — первого рода и $-a = -f(\alpha) = f(-\alpha)$ — натуральное число.

Теорема 2. *Кольцо целых чисел есть область целостности* (§ 7, определение 2) *с единицей, причём единицей служит натуральное число* 1.

Доказательство. Будем вместо a писать, если нужно, также $+a$. Покажем, что произведение ab целых чисел лишь тогда равно нулю, когда один из сомножителей равен нулю. Пусть $a \neq 0$ и $b \neq 0$. По предыдущей теореме $a = \pm c$ и $b = \pm d$, где c и d — натуральные числа. Тогда $ab = \pm cd$, где берём знак $+$ при одинаковых знаках a, b и знак $-$ при разных; $cd \neq 0$, так как произведение натуральных чисел является натуральным числом, следовательно, $ab \neq 0$.

Покажем, что $a \cdot 1 = a$ для любого a. Если a — натуральное число, то это верно по определению умножения (§ 13).

Если $a = 0$, то $a \cdot 1 = 0 \cdot 1 = 0 = a$. Если $a = -b$, где b — натуральное число, то $a \cdot 1 = (-b) \cdot 1 = -(b \cdot 1) = -b = a$. Теорема доказана.

Перейдём к понятиям о положительном и отрицательном числах и сравнению целых чисел по величине.

Теорема 3. *Кольцо целых чисел C может быть расположено* (§ 10, определение 1) *и притом единственным образом. При этом расположении все натуральные числа положительны, а все противоположные им числа* $-1, -2, -3, \ldots$ *— отрицательны.*

Доказательство. Если считать натуральные числа и только их за положительные, то кольцо C будет расположено. В самом деле, по теореме 1 для любого числа a либо a положительно, либо $a = 0$, либо $-a$ положительно, т. е. аксиома IX (§ 10) выполнена. Так как сумма и произведение натуральных чисел — числа натуральные, то выполнена и аксиома X. Раз натуральные числа положительны, то по самому определению противоположные им числа отрицательны. Покажем, что данное расположение — единственно возможное. Пусть кольцо C расположено каким угодно образом. По аксиоме IX одно из чисел $+1$ и -1 положительно. Тогда по аксиоме X число $1 = 1 \cdot 1 = (-1) \cdot (-1)$ как произведение положительных само положительно. Тогда также по аксиоме X и любое натуральное число n как сумма n единиц (§ 15, теорема 2) поло-

жительно, т. е. противоположное число $-n$ по аксиоме IX неположительно. По теореме 1 числа 0 и $\pm n$, где n — любое натуральное число, исчерпывают C. Таким образом в C положительны натуральные числа и только они. Итак, любое расположение C совпадает с расположением, указанным в начале доказательства.

Замечание 2. Целые числа обладают всеми свойствами элементов любого расположенного кольца, приведёнными в § 10. Так, считая $a > b$, если $a - b$ — положительно, мы вводим порядок, при котором 0 меньше всех положительных и больше всех отрицательных чисел (§ 10, теорема 1). Для этого порядка верны законы монотонности и правила оперирования с неравенствами (§ 10, теоремы 2—4). Определяя абсолютную величину $|a|$ числа a как неотрицательное из чисел $\pm a$ (см. § 10, определение 2), получим обычные её свойства и обычные правила сравнения и правила действий над числами через сравнение и действия над их абсолютными величинами (§ 10, теорема 8 и следующее за ней замечание).

Теорема 4. *Порядок натуральных чисел* (§ 14) *совпадает с их порядком в кольце целых чисел.*

Доказательство. Если a и b — целые числа и $a > b$, то $a - b = k$, где k — число положительное, т. е. натуральное, тогда $a = b + k$. Для натуральных a и b это означает, что $a > b$ в смысле определения из § 14.

Так как среди целых чисел нет наименьшего, то теорема 8 из § 14 для них уже неверна. Для справедливости утверждений такого рода необходимы дополнительные условия.

Определение. *Множество A целых чисел называется ограниченным сверху* (соответственно *снизу* или *просто ограниченным*), *если существует целое число k такое, что $k > x$* (соответственно $k < x$ или *существуют два числа k и l такие, что $k < x < l$*) *для любого числа x из A. Пустое множество ограничено.*

Теорема 5. *Любое непустое и ограниченное сверху* (соответственно *снизу* или *ограниченное*) *множество целых чисел A содержит наибольшее* (соответственно *наименьшее* или *как наибольшее, так и наименьшее*) *число.*

Доказательство. Пусть A ограничено сверху. Если A содержит хотя бы одно натуральное число, то множество натуральных чисел, входящих в A, непусто и содержит наибольшее число a (§ 14, теорема 2). Число a, очевидно, будет наибольшим и в A. Если A не содержит натуральных чисел, но оно содержит число 0, то 0 и будет наибольшим в A. Если A содержит лишь отрицательные числа, то множество B, содержащее числа, противоположные числам из A, состоит из натуральных чисел и содержит наименьший элемент b: $b \leqslant y$ для любого y из B. Умножая на -1, найдём (§ 10, теорема 2): $-b \geqslant -y$ или, полагая $a = -b$ и $x = -y$, $a \geqslant x$ для любого x из A. Если A ограничено снизу, то определённое выше B ограничено сверху, и по доказанному B содержит наи-

большее число b. Тогда число $a=-b$ будет наименьшим в A. Наконец, если A ограничено, то оно ограничено и сверху, и снизу, и по доказанному содержит как наибольшее, так и наименьшее число.

На этой теореме основаны различные формы односторонней или двусторонней индукции. Например:

Теорема 6. *Если некоторая теорема T, касающаяся целого числа, верна для целого числа a и*

а) *если из того, что теорема T верна для числа $x=a$, следует, что она верна для числа $x+1$, то она верна для любого числа $b\geqslant a$;*

б) *если из того, что теорема T верна для числа $x\leqslant a$, следует, что она верна для числа $x-1$, то она верна для любого числа $b\leqslant a$;*

в) *если из того, что теорема T верна для любого числа x, удовлетворяющего неравенству $x_1<x<x_2$, где $x_1\leqslant a\leqslant x_2$, следует, что она верна для чисел x_1 и x_2, то она верна для любого целого числа b.*

Доказательство. Все подобные утверждения доказываются одинаково. Докажем, например, утверждение в). Если теорема T верна не для всех целых чисел, то существует целое число b, для которого она неверна. Пусть $b>a$ (в случае $b<a$ рассуждение аналогично) и пусть A есть множество тех целых чисел $x>A$, для которых T неверна. Множество A ограничено снизу числом a и непусто, ибо содержит число b. По предыдущей теореме это множество содержит наименьшее число x_2. Если положим x_1 равно $a-1$, то теорема T верна для любого числа x такого, что $x_1<x<x_2$, причём $x_1<a<x_2$. Следовательно, теорема T верна и для чисел x_1 и x_2. Но число x_2 принадлежит множеству A, т. е. для x_2 теорема T неверна. Полученное противоречие доказывает утверждение в).

Теорема 7. *Кольцо целых чисел архимедовски расположено* (§ 10, определение 3).

Доказательство. Пусть a и b — целые числа и $b>0$. Если $a\leqslant 0$, то $1\cdot b=b>a$. Если $a>0$, то a и b — натуральные числа и для них аксиома Архимеда выполнена (§ 14, теорема 6). Поэтому существует натуральное число n такое, что $nb>a$.

На свойствах делимости целых чисел мы останавливаться не будем, так как они рассматриваются в статье А. Я. Хинчина.

ГЛАВА V

ПОЛЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ

§ 22. Определение поля рациональных чисел

В настоящей главе будут построены рациональные числа, положительные, отрицательные и число нуль. Дробные числа появились в глубокой древности задолго до отрицательных чисел. Их возникновение связано с задачами измерения. В случае, когда единица измерения не укладывалась целое число раз в измеряемой величине, естественно возникало понятие о дробном числе. Заметим, что принятый нами порядок изложения отличается от школьного тем, что мы сначала определяем целые отрицательные числа, а затем все рациональные числа, тогда как в школе отрицательные числа появляются уже после дробных. Такое построение нами принято с целью получить возможно раньше числовую область (целых чисел), которая является кольцом, с тем, чтобы далее применять общую теорию, построенную в главе II. Укажем, однако, на то, что без каких-либо существенных изменений в рассуждениях можно было бы переставить местами построения «относительных» чисел из § 20 и рациональных чисел из данного параграфа. Тем самым будет сохранён обычный для школы порядок изложения.

Расширение множества целых чисел до множества чисел рациональных производится по общему плану, указанному в § 18 для любого расширения, и рассуждения при этом аналогичны проведённым в § 20 при расширении натуральных чисел до целых. Всё отличие состоит в том, что тогда речь шла о свойствах сложения, а теперь — о свойствах умножения.

Во множестве целых чисел не всегда выполнима операция, обратная умножению, т. е. деление, даже при условии, что делитель отличен от нуля. Поставим задачу расширить кольцо C целых чисел до такого множества Г, где были бы заданы операции сложения и умножения, обладающие теми же свойствами, какими они обладали для целых чисел, причём деление на элементы множества, отличные от нуля кольца C, было бы всегда возможно. Это означает, что множество Г должно быть полем (§ 8, определение 1). Будем

искать минимальное из таких расширений в смысле следующего определения:

Определение 1. *Полем рациональных чисел называется минимальное поле* Г, *содержащее кольцо* C *целых чисел, т. е. множество, обладающее свойствами*:

1) Г *содержит* C; 2) Г *является полем*; 3) *сложение и умножение целых чисел совпадают с одноимёнными операциями над этими числами в поле* Г; 4) *поле* Г *не содержит отличного от него самого подполя, содержащего* C.

Элементы поля Г *называются рациональными числами.*

Из этого определения ещё неясно, существует ли такое поле и будет ли оно единственным. Покажем сначала, что поле рациональных чисел определено однозначно с точностью до изоморфизма.

Теорема 1. (Ср. § 20, теорема 1.) *Поле* Г, *содержащее кольцо* C *целых чисел* [1]), *тогда и только тогда будет полем рациональных чисел* (т. е. минимальным), *когда каждый его элемент равен частному целых чисел.*

Доказательство. а) Если поле Г содержит C и каждый элемент Г равен частному целых чисел, то Г минимально, так как любое подполе, содержащее Г, содержит и все частные целых чисел (§ 8, теорема 5) и совпадает с Г.

б) Пусть, обратно, поле Г минимально. Во всяком поле частное элементов обладает следующими свойствами (§ 8, теорема 3):

$$\left.\begin{array}{ll} \text{а)} & \text{если } b\neq 0,\ d\neq 0, \text{ то } \dfrac{a}{b}=\dfrac{c}{d} \\ & \text{тогда и только тогда, когда } ad=bc; \\ \text{б)} & \text{если } b\neq 0,\ d\neq 0, \text{ то } \dfrac{a}{b}\pm\dfrac{c}{d}=\dfrac{ad\pm bc}{bd}; \\ \text{в)} & \text{если } b\neq 0,\ d\neq 0, \text{ то } \dfrac{a}{b}\cdot\dfrac{c}{d}=\dfrac{ac}{bd}; \\ \text{г)} & \text{если } b\neq 0,\ c\neq 0,\ d\neq 0, \text{ то } \dfrac{a}{b}:\dfrac{c}{d}=\dfrac{ad}{bc}. \end{array}\right\} \quad (1)$$

Пусть M — множество всех элементов поля Г, каждый из которых равен частному целых чисел. Из (1) следует, что сумма, разность, произведение и частное (если делитель отличен от нуля) любых двух элементов множества M снова принадлежат к M, т. е. M — подполе поля Г (§ 8, теорема 5). Любое целое число равно, конечно, частному целых чисел, например $a=\frac{ab}{b}$, где b — целое число, отличное от нуля. Из совпадения операций в C и Г

[1]) Здесь и ниже подразумевается, что операции над элементами подмножества совпадают с одноимёнными операциями над теми же элементами в надмножестве.

следует поэтому, что M содержит C, и в силу минимальности Γ $M=\Gamma$. Это значит, что любое рациональное число равно частному целых чисел.

Теорема 2. (Ср. § 20, теорема 2.) *Все минимальные поля, содержащие кольцо C целых чисел, изоморфны, т. е. поле рациональных чисел единственно до изоморфизма.*

Доказательство. Пусть Γ_1 и Γ_2 — два таких поля. По предыдущей теореме любой элемент Γ_1 и Γ_2 равен частному целых чисел. Строим отображение f поля Γ_1 на Γ_2 так: если $c_1 \in \Gamma_1$, $c_1=\frac{a}{b}$ в Γ_1, где a и b — целые числа и $c_2=\frac{a}{b}$ в Γ_2, то положим $f(c_1)=c_2$. Ввиду полной аналогии дальнейших рассуждений с доказательством теоремы 2 из § 20 ограничимся лишь указанием, что взаимная однозначность этого отображения следует из свойства а). Далее, из свойства б) следует:

$$f(c_1+d_1)=f(c_1)+f(d_1),$$

и из в) следует

$$f(c_1d_1)=f(c_1)f(d_1)$$

для любых c_1 и d_1 из Γ, что и доказывает изоморфизм полей Γ_1 и Γ_2.

Теорема 3. (Ср. § 20, теорема 3.) *Любое поле P, содержащее кольцо целых чисел C, содержит и поле рациональных чисел.*

Доказательство. Пересечение всех подполей поля P, содержащих C, будет опять подполем (§ 8, теорема 6), содержащим C и при этом минимальным, так как оно входит в любое подполе, содержащее C. Согласно определению 1 это подполе будет полем рациональных чисел.

Переходим к доказательству существования поля рациональных чисел. Как и в случае кольца целых чисел, это доказательство проводится путём построения примера (интерпретации) поля, удовлетворяющего определению 1.

Конструкция одного из изоморфных полей рациональных чисел подсказывается теоремой 1. Ведь если Γ — поле рациональных чисел, то элементами Γ будут частные целых чисел. Правила сравнения и операции сложения и умножения для этих частных задаются формулами (1).

За исходный элемент построения поля рациональных чисел принимаем опять пару (a, b) целых чисел, взятых в данном порядке, причём второе число пары b отлично от нуля. Пусть M — множество всех таких пар. Определяем отношение эквивалентности, сложение и умножение пар так, чтобы им соответствовали равенства, сложения и умножения частных чисел этих пар в искомом поле. Именно, согласно (1) полагаем

$$(a, b)\sim(c, d) \qquad (2)$$

тогда и только тогда, когда $ad = bc$,

$$(a, b) + (c, d) = (ad + bc, bd), \tag{3}$$

$$(a, b)(c, d) = (ac, bd). \tag{4}$$

Отметим, что пары в правых частях (3) и (4) снова принадлежат множеству M, так как из $b \neq 0$ и $d \neq 0$ следует $bd \neq 0$ для любых целых чисел b и d (§ 21, теорема 2).

Теорема 4. *Сложение и умножение пар коммутативны, ассоциативны, а вместо закона дистрибутивности верна эквивалентность*

$$[(a, b) + (c, d)](e, f) \sim (a, b)(e, f) + (c, d)(e, f). \tag{5}$$

Доказательство. Все эти свойства доказываются непосредственной проверкой с использованием свойств целых чисел как элементов кольца (§ 20, определение 1). Проверим, например, эквивалентность (5). Преобразуем левую и правую части отдельно:

$$[(a, b) + (c, d)](e, f) = (ad + bc, bd)(e, f) = (a\,dc + bce, b\,df),$$

$$(a, b)(e, f) + (c, d)(e, f) = (ae, bf) + (ce, df) =$$
$$= (ae\,df + bfce, bf\,df).$$

Но из определения эквивалентности (2) следует, что получившиеся в итоге пары эквивалентны.

Отношение эквивалентности пар (2) обладает тремя основными свойствами равенства (§ 19), а именно:

1) $(a, b) \sim (a, b)$, ибо $ab = ba$;

2) если $(a, b) \sim (c, d)$, то $(c, d) \sim (a, b)$; ибо если $ad = bc$, то $cb = da$;

3) если $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$, то $(a, b) \sim (e, f)$, ибо умножая равенство $ad = bc$ на f и равенство $cf = de$ на b, находим: $adf = bcf = bde$, т. е. $adf = bde$, откуда $af = be$, так как $d \neq 0$.

Это отношение определяет разбиение множества M на классы эквивалентных пар. Будем обозначать эти классы малыми греческими буквами α, β, γ, δ, ...

Определение 2. *Пусть* Γ_0 *есть множество всех классов эквивалентных пар множества* M. *Суммой* (*произведением*) *двух классов* α *и* β *назовём тот класс* $\alpha + \beta$ (*соответственно*, $\alpha\beta$), *который содержит сумму* (*произведение*) *пары класса* α *и пары класса* β.

Как и в предыдущей главе, независимость суммы и произведения классов от выбора их представителей вытекает из такой теоремы:

Теорема 5. *Если* $(a_1, b_1) \sim (a_2, b_2)$ *и* $(c_1, d_1) \sim (c_2, d_2)$, *то*

$$(a_1, b_1) + (c_1, d_1) \sim (a_2, b_2) + (c_2, d_2)$$

и

$$(a_1, b_1)(c_1, d_1) \sim (a_2, b_2)(c_2, d_2).$$

Доказательство. Как и прежде (§ 20, теорема 5), достаточно доказать, что для любой пары (c, d) будет:

$$(a_1, b_1)+(c, d)\sim(a_2, b_2)+(c, d)$$

и

$$(a_1, b_1)(c, d)\sim(a_2, b_2)(c, d).$$

По условию эквивалентности (2) имеем:

$$a_1b_2=a_2b_1.$$

Умножим обе части на d. Найдём:

$$a_1b_2d=a_2b_1d.$$

Прибавим к обеим частям b_1cb_2. Получим:

$$a_1b_2d+b_1cb_2=a_2b_1d+b_1cb_2.$$

Умножим обе части снова на d и вынесем общие множители за скобки. Будем иметь:

$$(a_1d+b_1c)\,b_2d=(a_2d+b_2c)\,b_1d,$$

откуда

$$(a_1d+b_1c,\ b_1d)\sim(a_2d+b_2c,\ b_2d).$$

Умножим обе части равенства $a_1b_2=a_2b_1$ на cd. Найдём:

$$(a_1c)\,(b_2d)=(a_2c)\,(b_1d),$$

откуда

$$(a_1c,\ b_1d)\sim(a_2c,\ b_2d).$$

Итак, определение 2 действительно вводит во множестве Γ_0 классов эквивалентных пар однозначно определённые операции сложения и умножения.

Теорема 6. *Множество* Γ_0 *с операциями, указанными в определении* 2, *является полем.*

Доказательство. Нужно проверить выполнение в Γ_0 аксиом I—VI (§ 7, определение 1) и VII, VIII (§ 8, определение 1). Так как операции в Γ_0 определены для классов через их представителей, то выполнение аксиом I, II, IV, V и VI следует из теоремы 4. Так как, очевидно, множество Γ_0 содержит более одного элемента, то выполнена аксиома VIII. Выполнение аксиомы III следует из того, что если класс α содержит пару (a, b), класс β — пару (c, d), то из

$$(a, b)+(bc-ad,\ bd)=(abd+b^2c-abd,\ b^2d)\sim(c, d)$$

следует, что класс γ, содержащий пару $(bc-ad, bd)$, удовлетворяет условию $\alpha+\gamma=\beta$.

Итак, уже доказано, что Γ_0 является кольцом. Выясним, какой смысл имеют в этом кольце нуль и противоположный элемент. Все

пары вида $(0, b)$ эквивалентны между собой. Обратно, любая пара (x, y), эквивалентная паре $(0, b)$, сама имеет тот же вид, так как из $xb = y \cdot 0$ и $b \neq 0$ следует $x = 0$. Таким образом, все пары вида $(0, b)$ образуют один класс, который, очевидно, является нулём кольца Γ_0. Далее, очевидно, что противоположным для класса α, содержащего пару (a, b), является класс, содержащий пару $(-a, b)$. Будем его обозначать через $-\alpha$.

Проверим теперь выполнение аксиомы VII. Пусть даны классы α и β, причём класс α отличен от нуля. Если α содержит пару (a, b) и β — пару (c, d), то $a \neq 0$. Существует поэтому пара (bc, ad). Пусть γ — класс, содержащий эту пару. Из

$$(a, b)(bc, ad) = (abc, abd) \sim (c, d)$$

следует $\alpha\gamma = \beta$, что и доказывает VII. Итак, Γ_0 является полем.

Выясним ещё, какой смысл имеют в поле Γ_0 единица и обратный элемент. Если $\alpha\varepsilon = \alpha$, где α отлично от нуля, α содержит (a, b), где $a \neq 0$, ε содержит (x, y), то $(a, b)(x, y) \sim (a, b)$, откуда $abx = aby$, $x = y$. Очевидно, что, обратно, пара вида (x, x), $x \neq 0$ удовлетворяет условию

$$(a, b)(x, x) \sim (a, b).$$

Все пары этого вида составляют один класс, играющий, очевидно, роль единицы в поле Γ_0.

Обратным для класса α, содержащего пару (a, b), $a \neq 0$, будет класс, содержащий пару (b, a), так как $(a, b)(b, a) = (ab, ab)$ принадлежит единичному классу.

Построенное поле Γ_0 является изоморфным полю рациональных чисел. Само поле Γ_0 не удовлетворяет определению 1, так как не содержит среди своих элементов целых чисел.

Займёмся теперь включением в поле Γ_0 кольца целых чисел. Сначала найдём в поле Γ_0 множество, изоморфное кольцу целых чисел C. Пусть класс α содержит пару (b, c), где b делится на c, т. е. $b = ac$. Очевидно, что две пары вида (ac_1, c_1) и (ac_2, c_2) эквивалентны. Обратно, всякая пара, эквивалентная паре (ac, c), сама будет вида (ac_1, c_1). В самом деле, из $(b_1, c_1) \sim (ac, c)$ следует: $b_1 c = c_1 ac$, откуда $b_1 = ac_1$. Итак, класс α состоит из пар вида (ac, c) с данным a и любым $c \neq 0$.

Пусть C' — множество всех классов пар (b, c), где b делится на c. Каждому классу α из C' поставим в соответствие число a такое, что пара (ac, c) принадлежит этому классу α. Так как $(ac_1, c_1) \sim (ac_2, c_2)$, то этим определено однозначное отображение $a = f(\alpha)$ множества классов C' во множество целых чисел C. Двум разным классам соответствуют разные числа, и любое число a соответствует некоторому классу, именно классу, содержащему пару (ac, c). Таким образом, f есть взаимно однозначное отображение C' на C.

Покажем, что f будет изоморфным отображением множества C' с операциями над классами на кольцо целых чисел. Достаточно доказать равенства

$$f(\alpha)+f(\beta)=f(\alpha+\beta), \quad f(\alpha)\cdot f(\beta)=f(\alpha\beta). \tag{6}$$

Но если класс α содержит пару $(ac,\ c)$ и класс β — пару $(bc,\ c)$, то $(\alpha+\beta)$ содержит пару

$$(ac,\ c)+(bc,\ c)=[(a+b)c^2,\ c^2]$$

и класс $\alpha\beta$ — пару

$$(ac,\ c)(bc,\ c)=(abc^2,\ c^2),$$

откуда

$$f(\alpha+\beta)=a+b=f(\alpha)+f(\beta)$$

и

$$f(\alpha\beta)=ab=f(\alpha)\cdot f(\beta).$$

Построим теперь искомое поле рациональных чисел Г. Пусть Г — множество, полученное из поля Γ_0 путём замены каждого класса множества C' соответствующим ему при отображении f целым числом. Для определения операций в Г дополним определение отображения f, положив $f(\alpha)=\alpha$ для любого класса из Γ_0, не входящего в C'. Тогда f будет взаимно однозначным отображением Γ_0 на Г. Сложение и умножение в Г определяем равенствами

$$f(\alpha)+f(\beta)=f(\alpha+\beta), \quad f(\alpha)\cdot f(\beta)=f(\alpha\beta). \tag{7}$$

Здесь α и β — любые элементы Γ_0, следовательно $f(\alpha)$ и $f(\beta)$ — любые элементы Г. Поэтому равенствами (7) действительно определены операции во множестве Г.

Теорема 7. *Множество* Г *с операциями, определёнными равенствами* (7), *является полем рациональных чисел.*

Доказательство. Надо показать, что множество Г обладает свойствами 1)—4) из определения 1.

1) Г содержит кольцо целых чисел C по построению.

2) Г является полем, так как равенства (7), определяющие сложение и умножение в Г, вместе с тем показывают, что множество Г относительно этих операций изоморфно полю Γ_0. Но множество с двумя операциями, изоморфное полю, само является полем (§ 9, теорема 1).

3) Сложение и умножение целых чисел совпадают с одноимёнными операциями над этими числами в поле Г. В самом деле, при отображении f целые числа являются образами элементов множества C' из поля Г. Но если α и β — классы из C', то для них равенства (7) совпадают с (6), где сложение и умножение в левых частях равенств означают операции над целыми числами, определённые в § 20.

4) Поле Γ не содержит отличного от него самого подполя, содержащего C. Чтобы в этом убедиться, покажем, что любой элемент поля Γ равен частному целых чисел. Любой элемент из Γ имеет вид $f(\alpha)$, где α — некоторый класс поля Γ_0.

Пусть класс α содержит пару (k, l) целых чисел, причём $l \neq 0$. Тогда $k = f(\beta)$, $l = f(\gamma)$. По определению отображения f класс β состоит из пар вида (kc, c) и γ — из пар вида (lc, c), следовательно класс $\alpha\gamma$ содержит пару

$$(k, l)(lc, c) = (klc, lc) \sim (kc, c),$$

откуда $\alpha\gamma = \beta$. Согласно определению умножения в Γ [второе из равенств (7)] отсюда находим: $f(\alpha) \cdot f(\gamma) = f(\beta)$, откуда

$$f(\alpha) = \frac{f(\beta)}{f(\gamma)} = \frac{k}{l}.$$

Любое подполе поля Γ, содержащее все целые числа, должно содержать и все их частные, т. е. по доказанному всё поле Γ, чем и завершается доказательство теоремы.

Итак, одно из изоморфных полей рациональных чисел нами построено. Его элементами являются, во-первых, все целые числа и, во-вторых, классы эквивалентных пар целых чисел вида (a, b), где $b \neq 0$ и a не делится на b. Этим решён вопрос о существовании поля рациональных чисел, т. е. поля, удовлетворяющего определению 1. Остаётся ввести для рациональных чисел обычные обозначения с помощью дробей и показать, что эти числа обладают обычными, всем известными, свойствами.

§ 23. Свойства рациональных чисел

Введём для рациональных чисел, рассматриваемых как элементы построенного в предыдущем параграфе поля Γ, обычные обозначения с помощью дробей. Каждое рациональное число a является образом некоторого класса α поля Γ_0, т. е. $a = f(\alpha)$. Класс α однозначно определяется любой входящей в него парой (k, l) целых чисел, где $l \neq 0$. Таким образом, любое рациональное число a однозначно определяется парой (k, l) из класса α. Будем обозначать это число a через $\frac{k}{l}$, а символы $\frac{k}{l}$, где k и l — целые числа и $l \neq 0$, будем называть *дробями* [1]).

---

[1]) Таким образом, в отличие от молчаливо принимаемого обычно понимания дробей как чисел особой категории мы считаем дроби не числами, а лишь символами для обозначения чисел. В самом деле, различные дроби могут обозначать одно и то же число. Так,

$$\frac{2}{3} = \frac{4}{6} = \frac{6}{9} = \ldots$$

Но тот же символ $\frac{k}{l}$ в поле Г обозначает частное от деления k на l. Это не ведёт, однако, к противоречию, так как по доказанному в конце предыдущего параграфа, если $a=f(\alpha)$ и класс α содержит пару (k, l), то действительно $a=\frac{k}{l}$, где $\frac{k}{l}$ — частное от деления k на l.

Все дроби, составленные из пар одного класса α, обозначают одно и то же рациональное число $a=f(\alpha)$. Таким образом, по определению эквивалентности пар (2) имеем

$$\frac{a}{b}=\frac{c}{d} \tag{1}$$

тогда и только тогда, когда $ad=bc$.

Отсюда, в частности, вытекает основное свойство дроби, т. е. равенство

$$\frac{a}{b}=\frac{ac}{bc} \tag{2}$$

для любого $c\neq 0$. На этом свойстве основаны, как известно, сокращение дробей и приведение дробей к общему знаменателю.

Заметим, что $a=\frac{k}{l}$ будет целым при условии, что k делится на l. Простейшим обозначением целого числа a дробью будет дробь $\frac{a}{1}$. Для целых чисел мы будем применять наряду с дробями также и прежние обозначения. Так,

$$\frac{6}{3}=\frac{4}{2}=\frac{2}{1}=2, \quad \frac{-15}{3}=\frac{-5}{1}=-5.$$

Так как дробь $\frac{k}{l}$ обозначает рациональное число, равное частному от деления k на l в поле Г, то для действий сложения, вычитания, умножения и деления над числами, обозначенными дробями, верны правила (1), б), в), г) § 22, т. е. обычные правила оперирования с дробями.

Рациональные числа, не являющиеся целыми, будем называть *дробными* (таким образом, мы будем различать термины «дробь» и «дробное число»). Итак, целые и дробные числа вместе составляют все рациональные числа.

Замечание 1. Для рациональных чисел как элементов поля Г верны все теоремы, доказанные для любых колец и полей в §§ 7, 8. Так, верны правила знаков при умножении [§ 7, (3)]; существует единица, причём она равна числу 1, соответствующему единичному классу поля Γ_0 при изоморфном отображении f (ибо этот класс состоит из пар вида $(c, c)=(c\cdot 1, c)$, где $c\neq 0$); любое число $\frac{a}{b}\neq 0$ имеет обратное, причём это будет число $\frac{b}{a}$; отсутствуют делители нуля (§ 8, теорема 1) и т. д.

Переходим к свойствам расположения поля рациональных чисел.

Теорема 1. *Поле* Г *рациональных чисел может быть расположено* (§ 10, определение 1) *и притом единственным образом. При этом число* $a=\frac{k}{l}$ *положительно, если целое число* kl *положительно. Это расположение в частном случае целых чисел совпадает с расположением целых чисел, определённым ранее* (§ 21, теорема 3).

Доказательство. Будем считать рациональное число $a=\frac{k}{l}$, где $k\neq 0$, положительным, если целые числа k и l — одного знака, т. е. или оба положительны, или оба отрицательны, иначе говоря, $a=\frac{k}{l}$ положительно (в символах: $a>0$), если $kl>0$ в смысле расположения целых чисел. Это определение положительности числа a не зависит от его записи в виде дроби. В самом деле, если $a=\frac{k_1}{l_1}=\frac{k_2}{l_2}$ и $k_1l_1>0$, то, умножая последнее неравенство на положительное целое число l_2^2, получим:

$$k_1l_1l_2^2=(k_1l_2)(l_1l_2)=(k_2l_1)(l_1l_2)=k_2l_2l_1^2>0.$$

Но $l_1^2>0$, следовательно $k_2l_2>0$ (§ 10, теорема 3).

Покажем, что данное определение положительных чисел удовлетворяет аксиомам IX и X из § 10. Пусть $a=\frac{k}{l}$. Так как для целых чисел аксиома IX выполнена, то выполнено одно и только одно из трёх соотношений $kl>0$, $kl=0$, $-kl>0$.

Если $kl>0$, то $a>0$, если $kl=0$, то $k=0$ и $a=0$, если $-kl>0$, то $-a=\frac{-k}{l}>0$. Итак, аксиома IX справедлива и для рациональных чисел. Если

$$a_1=\frac{k_1}{l_1}>0 \quad \text{и} \quad a_2=\frac{k_2}{l_2}>0,$$

то

$$a_1+a_2=\frac{k_1l_2+k_2l_1}{l_1l_2}>0,$$

ибо

$$(k_1l_2+k_2l_1)\,l_1l_2=(k_1l_1)\,l_2^2+(k_2l_2)\,l_1^2>0.$$

А также

$$a_1a_2=\frac{k_1k_2}{l_1l_2}>0,$$

ибо

$$(k_1k_2)(l_1l_2)=(k_1l_1)(k_2l_2)>0.$$

Итак, аксиома X для рациональных чисел выполнена. Поле Г расположено.

Легко видеть, что аксиомы IX и X, выполненные для некоторого кольца или поля, остаются справедливыми для любого его подкольца. Поэтому расположение поля Γ рациональных чисел порождает некоторое расположение содержащегося в нём кольца C целых чисел. Но кольцо целых чисел допускает единственное расположение (§ 21, теорема 3). Поэтому любое расположение (в частности, определённое выше) поля рациональных чисел сохраняет расположение кольца целых чисел, определённое ранее (§ 21).

Покажем, что построенное расположение поля рациональных чисел является единственным. Пусть дано какое-то его расположение. Оно сохраняет неизменным расположение целых чисел. Покажем, что рациональное число $a=\frac{k}{l}$ тогда и только тогда положительно, когда целое число kl положительно. В самом деле, если $\frac{k}{l}>0$, то, умножая на $l^2>0$, найдём $kl>0$. Если, обратно, $kl>0$, то и $\frac{k}{l}>0$, так как иначе $-\frac{k}{l}\geqslant 0$, и, умножая на $l^2>0$, найдём $-kl\geqslant 0$, что противоречит $kl>0$.

Итак, любое расположение поля рациональных чисел совпадает с определённым в начале доказательства. Теорема доказана.

Замечание 2. Рациональные числа обладают всеми свойствами элементов любого расположенного поля, приведёнными в § 10. Так, считая $a>b$, если $a-b$ положительно, мы вводим порядок, при котором 0 меньше всех положительных и больше всех отрицательных чисел (§ 10, теорема 1). Для этого порядка верны законы монотонности и правила оперирования с неравенствами (§ 10, теоремы 2—4). Поле рациональных чисел имеет характеристику 0 (§ 10, теорема 6). Определяя абсолютную величину числа a как неотрицательное из чисел $\pm a$, получим обычные её свойства, в том числе обычные правила сравнения двух чисел по величине и правила четырёх арифметических действий через действия над абсолютными величинами (§ 10, теорема 8 и следующие за ней замечания).

Пусть P — любое поле характеристики 0 (§ 8, определение 2) и e — единица поля P. Определим произведение ax любого элемента x поля P на любое рациональное число a. Если $a=\frac{k}{l}$ с целыми k, l и $l\neq 0$, то и $le\neq 0$, и мы положим:

$$ae=\frac{k}{l}e=\frac{ke}{le},\quad ax=(ae)x.$$

Для целого a это определение совпадает с данным в § 7, ибо из $a=\frac{k}{l}$ следует $al=k$ и по (5) из § 7

$$(ae)(le)=(al)e=ke,$$

откуда $ae=\frac{ke}{le}$. Тогда $(ae)x=a(ex)=ax$, т. е. произведение ax в новом смысле при целом a совпадает с произведением в смысле § 7.

Элементы ae при целом a называются *целыми*, а при рациональном a — *рациональными элементами поля* P.

Теорема 2. *Любое поле* Q *характеристики* 0 *содержит одно и только одно подполе* Π, *изоморфное полю рациональных чисел* Γ. *Это подполе* Π *состоит из всех рациональных элементов* ae *поля* Q, *и существует только одно изоморфное отображение* Π *на* Γ, *а именно, переводящее элемент* ae *в число* a. *В частности, поле* Γ *не имеет отличных от него самого подполей, т. е. является простым полем* (§ 8, определение 2) *и допускает лишь одно изоморфное отображение на себя, а именно, тождественное. Поле* Q *изоморфно полю* P, *содержащему* Γ *в качестве подполя, причём любое изоморфное отображение* Q *на* P *сохраняет указанное выше отображение* Π *на* Γ. *Если поле* Q *расположено, то и поле* P *может быть расположено так, что изоморфизм* P *и* Q *сохраняет отношение порядка.*

Доказательство. Для любых целых чисел m и n имеем [§ 6, (6) и § 7 (5)]:

а) $$me+ne=(m+n)e, \qquad (me)(ne)=(mn)e.$$

Так как характеристика поля Q равна нулю, то $ne\neq 0$ для любого целого $n\neq 0$. Если $m\neq n$, то $m-n\neq 0$ и $me-ne=(m-n)e\neq 0$. Таким образом, соответствие $n\longleftrightarrow ne$ между кольцом C целых чисел и множеством S целых элементов поля Q взаимно однозначно и в силу а) изоморфно.

Точно так же из соотношений а) и правил сложения и умножения частных б), в) (§ 8, теорема 3) имеем для любых рациональных $a=\frac{k}{l}$ и $b=\frac{m}{n}$ равенства

б) $$ae+be=(a+b)e, \qquad (ae)(be)=(ab)e,$$

ибо

$$ae+be=\frac{ke}{le}+\frac{me}{ne}=\frac{(ke)(ne)+(le)(me)}{(le)(ne)}=\frac{(kn+lm)e}{(ln)e}=(a+b)e,$$

$$(ae)(be)=\frac{ke}{le}\cdot\frac{me}{ne}=\frac{(ke)(me)}{(le)(ne)}=\frac{(km)e}{(ln)e}=(ab)e.$$

Если $a=\frac{k}{l}\neq 0$, то $k\neq 0$ и $ae=\frac{ke}{le}\neq 0$.

Отсюда, как выше, если $a\neq b$, то $ae\neq be$, и, следовательно, отображение $a\longleftrightarrow ae$ поля Γ на множество Π взаимно однозначно и в силу б) изоморфно. Так как Γ — поле, то и Π будет полем (§ 9, теорема 1). Пусть поле Γ каким угодно образом отображено изоморфно на некоторое подполе Π' поля Q. Числу 1 соответствует тогда единица e из Q, а потому по свойствам изоморфизма для

натурального n также

$$n = 1 + \cdots + 1 \longleftrightarrow e + \cdots + e = ne$$

и

$$-n \longleftrightarrow -ne = (-n)e, \quad 0 \longleftrightarrow 0 = 0 \cdot e$$

(0 слева — число, а справа — элемент Q). Итак, $n \longleftrightarrow ne$ для любого целого n. А тогда для любого рационального $a = \frac{m}{n}$ также $a = \frac{m}{n} \longleftrightarrow \frac{me}{ne} = ae$. Таким образом, Π' совпадет с Π, и любой изоморфизм между Γ и Π совпадает с изоморфизмом $a \longleftrightarrow ae$.

Так как поле Q содержит подполе Π, изоморфное Γ, то оно изоморфно полю P, содержащему подполе Γ и полученному из Q путём замены элементов Π соответствующими им числами из Γ (§ 9, теорема 2). При этом любой изоморфизм P и Q должен сохранять данный изоморфизм Γ и Π, так как Γ только одним способом изоморфно отображается в Π.

Если поле Q расположено и $y = f(x)$ — любое изоморфное отображение P на Q, то, считая элемент x из P положительным, если соответствующий ему элемент $y = f(x)$ из Q положителен, получим, как легко видеть, расположение поля P, причём изоморфизм f сохраняет отношения порядка. Теорема доказана.

Эта теорема показывает, что поле рациональных чисел в известном смысле является минимальным среди всех полей характеристики нуль. Именно, если изучать поля лишь с точностью до изоморфизма, то можно сказать, что любое поле характеристики нуль содержит в качестве подполя поле рациональных чисел.

Теорема 3. *Поле* Γ *рациональных чисел архимедовски расположено* (при единственно возможном его расположении).

Доказательство. Для выполнения аксиомы Архимеда в Γ, как и в любом расположенном поле, достаточно, чтобы для любого числа c существовало натуральное число n, большее c. В самом деле, тогда для любых a и b, где $b > 0$, существует $n > \frac{a}{b}$, и, умножая на b, получим $nb > a$.

Пусть a — любое рациональное число. Если $a \leqslant 0$, то $n > a$ для любого натурального n. Если $a > 0$, то его можно представить дробью $a = \frac{k}{l}$, где k и l — натуральные числа, ибо по теореме 1 $kl > 0$, т. е. k и l одного знака, а по (2) знаки k и l можно менять одновременно. Тогда $l \geqslant 1$, и, умножая на $a > 0$, найдём $k \geqslant a$, откуда $n = k + 1 > a$. Теорема доказана.

Теория делимости для поля рациональных чисел, как и для всякого поля, бессодержательна и сводится к положению, что любое число делится на любое другое число, отличное от нуля.

Для применения математики в технике и других науках в известном смысле слова достаточно одних рациональных чисел и даже не

всех рациональных чисел, а, например, чисел, выражаемых конечными десятичными дробями. В самом деле, во всех измерениях и вычислениях прикладного характера достаточно знать результат вычисления лишь с некоторой определённой степенью точности. При этом нужной точности можно достигнуть, используя лишь числа указанного рода. Для точного уяснения смысла этого утверждения введём такое понятие.

Определение. *Пусть дано натуральное число n. Все рациональные числа вида mn^k, где m и k — любые целые числа, называются n-ично рациональными или n-рациональными.*

При $n=2$, 3, 10 получим двоично-рациональные, троично-рациональные или десятично-рациональные (т. е. десятичные дроби) числа.

При $k=0$ найдём, что все целые числа n-рациональны для любого n.

То, что для всех приближённых вычислений рациональные числа можно заменить n-рациональными, вытекает из следующих двух предложений, которые мы докажем не для поля рациональных чисел Г, а в более общем виде, так как в этом виде они нам понадобятся в следующей главе.

Теорема 4. *Пусть P — архимедовски расположенное поле, содержащее поле рациональных чисел Г, a — элемент P и n — натуральное число, большее единицы. Тогда для любого целого числа k существует целое число m такое, что*

$$mn^k \leqslant a < (m+1)\,n^k.$$

Доказательство. Из $n>1>0$ следует $n^k>0$. Так как поле P архимедовски расположено, то существуют натуральные числа l_1 и l_2 такие, что $l_1 n^k > a$ и $l_2 n^k > -a$, откуда $(-l_2)\,n^k < a$. Следовательно, множество A целых чисел l, для которых $ln^k \leqslant a$, содержит $-l_2$, т. е. непусто, и ограничено сверху, так как из $ln^k \leqslant a < l_1 n^k$ следует $l < l_1$. Поэтому A содержит наибольшее число m (§ 21, теорема 5). Так как m принадлежит A и $m+1>m$ уже не принадлежит A, то по определению множества A имеем:

$$mn^k \leqslant a < (m+1)\,n^k,$$

что и требовалось доказать.

Теорема 5. *Пусть P — архимедовски расположенное поле, содержащее поле рациональных чисел Г, n — натуральное число, большее единицы. Для любого положительного элемента a поля P существует натуральное число k такое, что* $\frac{1}{n^k} < a$.

Доказательство. Сначала докажем неравенство

$$n^k > k \tag{3}$$

для любого натурального числа $n>1$ и любого целого числа k.

Так как $n^k > 0$, то для $k \leqslant 0$ это неравенство выполнено. Для натурального k докажем его индукцией по числу k при данном n. По условию $n^1 = n > 1$, т. е. для $k = 1$ неравенство верно. Если оно верно для числа k, то $n^k > k$, откуда

$$n^{k+1} = n \cdot n^k > nk \geqslant 2k = k + k \geqslant k + 1,$$

т. е. неравенство верно и для числа $k + 1$. Так как $a > 0$, то по аксиоме Архимеда найдётся натуральное число k, для которого $1 < ka$. По (3) тогда также $1 < n^k a$. Умножая на $n^{-k} > 0$, найдём $n^{-k} < a$, что и требовалось доказать.

Заметим, что ввиду теоремы 2 последние две теоремы остаются верными для любого архимедовски расположенного поля P с заменой в их формулировках рациональных чисел на соответствующие им элементы (т. е. числа r на элемент re, где e — единица P).

Из теорем 4 и 5 вытекает, что для целей приближённых вычислений рациональные числа можно заменить n-рациональными при данном n. В частности, можно применять числа, изображаемые конечными десятичными дробями ($n = 10$), что и делают на практике. В самом деле, мы скажем, что результат вычисления найден при помощи рациональных чисел с точностью до данного рационального числа $c > 0$, если найдены два рациональных числа a и b (результаты вычисления по недостатку и по избытку) такие, что $a < b$, $b - a < c$ и искомый результат вычисления заключён (в определённом смысле для данного вычисления) между a и b. Но по теореме 5 существует целое k такое, что

$$n^k < \frac{c - (b - a)}{2}.$$

Далее, по теореме 4 найдутся целые числа l и m такие, что

$$a_1 = ln^k \leqslant a < (l + 1)\, n^k \quad \text{и} \quad (m - 1)\, n^k \leqslant b < mn^k = b_1.$$

Так как интервал (a_1, b_1) шире (a, b), то естественно считать результат вычисления заключённым между a_1 и b_1. Далее,

$$b_1 - a_1 = (b_1 - b) + (b - a) + (a - a_1) \leqslant$$
$$\leqslant n^k + (b - a) + n^k < (b - a) + 2\,\frac{c - (b - a)}{2} = c.$$

Таким образом, a_1 и b_1 служат приближениями по недостатку и по избытку с помощью n-рациональных чисел с тою же степенью точности c. Рассуждая аналогично, можно и число c заменить меньшим уже n-рациональным числом.

Однако для точного выражения результата вычисления недостаточно не только n-рациональных, но и всех рациональных чисел.

Пусть, например, надо найти длину отрезка MN, если отрезок AB принят за единицу измерения. Искомая длина есть отношение отрез-

ков MN и AB. Если отрезки AB и MN соизмеримы, то имеется их общая мера CD, содержащаяся p раз в MN и q раз в AB. Тогда $MN:AB=\frac{p}{q}$ — число рациональное. Обратно, если отношение $MN:AB=\frac{p}{q}$ — рационально, то делим отрезок AB на q частей (одна из них p раз уложится в MN), следовательно MN и AB будут соизмеримы. Из геометрии известно, что существуют несоизмеримые отрезки. Так, диагональ квадрата несоизмерима с его стороной. Приняв стороны квадрата за единицу измерения отрезков, мы не можем выразить длину его диагонали никаким рациональным числом.

Рациональных чисел недостаточно также для извлечения корней из положительных рациональных чисел и даже из натуральных чисел. В самом деле, если, например, p — простое число, n — натуральное число, большее единицы, то $\sqrt[n]{p}$ не может равняться рациональному числу. Иначе, $\sqrt[n]{p}=\frac{q}{r}$ с натуральными q, r (если для чётного n взять положительное значение корня). Тогда $p=\frac{q^n}{r^n}$ и

$$pr^n=q^n. \tag{4}$$

Если в разложении числа q на простые множители p встречается a раз, а в разложении числа r встречается b раз, то в левой части равенства (4) p войдёт множителем $na+1$, а в правой части — nb раз. Но $na+1\neq nb$, так как второе число делится на n, а первое не делится. Таким образом, в разложении на простые множители левой и правой частей равенства (4) простое число p входит неодинаковое число раз, что противоречит однозначности разложения натурального числа на простые множители [1]).

В следующей главе мы займёмся расширением поля рациональных чисел до поля действительных чисел, в котором измерение отрезков и извлечение корня из положительного числа дают точный результат.

---

[1]) См. статью А. Я. Хинчина.

ГЛАВА VI

ПОЛЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

§ 24. Полные и непрерывные поля

Ещё в Древней Греции было известно существование несоизмеримых отрезков. Стремление получить для их отношения точное числовое значение должно было бы привести к понятию иррационального числа. Однако строгое обоснование этого понятия оказалось не под силу учёным древности. Стремясь к строгому обоснованию математических положений, они придавали им геометрическую форму. Примером этой своеобразной геометрической алгебры могут служить «Начала» Евклида.

В Средние века индусы пользовались иррациональными выражениями, не вдаваясь в вопросы их обоснования. С развитием анализа в XVII и XVIII вв. действительные числа становятся основным объектом исследования. При этом с ними оперировали на основе наглядных представлений, изображая числа точками прямой линии.

Ко второй половине XIX в. потребность формального построения теории действительного числа назрела настолько, что она была построена рядом математиков (Дедекинд, Кантор, Вейерштрасс). Все эти построения, по форме совершенно различные, равноправны в том смысле, что приводят к изоморфным числовым областям. Мы приведём ниже построение Кантора как наиболее тесно связанное с понятием предела, рассмотренным выше. В литературе чаще встречается построение Дедекинда, с которым читатель может познакомиться по книге самого автора [10]; прекрасное изложение теории Дедекинда, богатое ценными методологическими указаниями, дано в книге А. Я. Хинчина [11].

Как было показано в конце § 23, отношение отрезков и корень из положительного рационального числа не всегда выражаются рациональными числами. Мы хотим теперь расширить поле рациональных чисел Γ до поля действительных чисел D, в котором эти задачи (а также широкий класс других задач) были бы всегда разрешимы.

Чтобы понять, какие свойства чисел нужны для разрешимости этих задач, и притти тем самым к целесообразному определению поля действительных чисел, разберём эти две задачи подробнее.

Пусть надо найти отношение отрезков AB и MN. Тогда мы откладываем на отрезке MN от точки M отрезок $MM_1 = AB$, затем от M_1 в том же направлении $M_1M_2 = AB$ и т. д. По геометрической аксиоме Архимеда найдётся натуральное число n такое, что, отложив таким образом n раз отрезок AB, мы получим отрезок $n \cdot AB > MN$. Таким образом, множество тех целых чисел k, для которых $k \cdot AB \leqslant MN$, ограничено сверху и непусто, ибо число 0 ему принадлежит. Поэтому это множество содержит наибольшее число a_0 (§ 21, теорема 5). Если $a_0 + 1 = b_0$, то

$$a_0 \cdot AB \leqslant MN < b_0 \cdot AB.$$

Естественно считать, что искомое отношение $MN : AB$ лежит между a_0 и b_0. Далее, делим AB на 10 равных частей и для одной из них A_1B_1 повторяем наше рассуждение. Получим целые числа a_1' и $b_1' = a_1' + 1$, для которых,

$$a_1' \cdot A_1B_1 \leqslant MN < b_1' \cdot A_1B_1,$$

или, полагая

$$a_1 = \frac{a_1'}{10}, \quad b_1 = \frac{b_1'}{10},$$

имеем:

$$a_1 \cdot AB \leqslant MN < b_1 \cdot AB, \quad b_1 - a_1 = \frac{1}{10}.$$

Так как

$$10a_0 \cdot A_1B_1 = a_0 \cdot AB \leqslant MN < b_0 \cdot AB = 10b_0 \cdot A_1B_1,$$

то по максимальности a_1' будем иметь:

$$10a_0 \leqslant a_1' < 10b_0,$$

откуда

$$b_1' = a_1' + 1 \leqslant 10b_0$$

и

$$a_0 \leqslant \frac{a_1'}{10} = a_1 \quad \text{и} \quad b_0 \geqslant \frac{b_1'}{10} = b_1.$$

Повторяя те же рассуждения, получим две последовательности чисел a_n и b_n, удовлетворяющие условиям

$$\left.\begin{array}{ll} \text{а)} & a_0 \leqslant a_1 \leqslant a_2 \leqslant \ldots, \\ \text{б)} & b_0 \geqslant b_1 \geqslant b_2 \geqslant \ldots, \\ \text{в)} & b_n - a_n = \dfrac{1}{10^n}, \quad n = 0, 1, 2, \ldots \end{array}\right\} \qquad (1)$$

Искомое отношение отрезков MN и AB естественно считать лежащим между a_n и b_n. Числа каждой из этих последовательностей всё более приближаются к этому отношению. Каково бы ни было данное положительное рациональное число ε, можно найти такое натуральное число n_0, что числа a_n и b_n различаются между собой (а значит, и от искомого отношения) меньше чем на ε при любом $n > n_0$. В самом деле, существует n_0, для которого $\frac{1}{10^{n_0}} < \varepsilon$ (§ 23, теорема 5), а потому $b_n - a_n = \frac{1}{10^n} < \varepsilon$ при $n > n_0$.

Пусть надо найти $\sqrt[k]{a}$, где a — положительное рациональное и $k > 1$ — натуральное число. Будем говорить лишь о положительном значении корня. Берём любое целое число $n \geqslant 0$. Так как $10^{-n} > 0$, то по аксиоме Архимеда существует натуральное число m такое, что $m \cdot 10^{-n} > a + 1$. Для любого рационального $b > 1$ и любого натурального $k > 1$ имеем: $b^{k-1} > 1$ (§ 10, теорема 4), откуда $b^k > b$. Поэтому

$$(m \cdot 10^{-n})^k > m \cdot 10^{-n} > a + 1 > a.$$

Множество A тех целых чисел l, для которых $(l \cdot 10^{-n})^k \leqslant a$, ограничено сверху и непусто, так как содержит число 0. Поэтому оно содержит наибольшее число a'_n. Если

$$b'_n = a'_n + 1, \quad a_n = a'_n \cdot 10^{-n}, \quad b_n = b'_n \cdot 10^{-n},$$

то

$$a_n^k \leqslant a < b_n^k.$$

Естественно считать, что искомый корень $\sqrt[k]{a}$ лежит между a_n и b_n. Далее, $b_n - a_n = 10^{-n}$. Так как числа вида $m \cdot 10^{-n}$ являются также числами вида

$$m' \cdot 10^{-(n+1)},$$

то

$$a_n = a'_n \cdot 10^{-n} = 10 \cdot a'_n \cdot 10^{-(n+1)} \leqslant a'_{n+1} \cdot 10^{-(n+1)} = a_{n+1}.$$

Так как

$$a < (b'_n \cdot 10^{-n})^k = (10 \cdot b'_n \cdot 10^{-(n+1)})^k,$$

то

$$a'_{n+1} < 10 \cdot b'_n,$$

откуда

$$b'_{n+1} = a'_{n+1} + 1 \leqslant 10 \cdot b'_n,$$

$$b_{n+1} = b'_{n+1} \cdot 10^{-(n+1)} \leqslant 10 \cdot b'_n \cdot 10^{-(n+1)} = b_n.$$

Итак, мы снова получаем последовательности a_n и b_n с теми же свойствами (1). Мы принимаем, что искомый корень при любом n лежит между a_n и b_n. О приближении этих чисел к значению корня можно сказать точно то же самое, что было сказано в случае отношения отрезков.

Всё дело заключается, однако, в том, что такого числа, к которому числа a_n и b_n приближались бы вышеописанным образом, среди рациональных чисел может не быть. Для того чтобы такое число нашлось для любых последовательностей рациональных чисел a_n и b_n со свойствами (1), приходится вводить новые (нерациональные) числа. Для их введения надо точно определить понятие последовательности и её свойства.

Определение 1. *Последовательностью элементов данного непустого множества M называется функция* (§ 3, определение 1) $f(n)=a_n$, *определённая на множестве N всех натуральных чисел, значение которой принадлежит множеству M.* Иными словами, *последовательностью называется всякое соответствие, сопоставляющее с каждым натуральным числом n некоторый элемент a_n множества M.*

Последовательность обозначается символами $a_1, a_2, a_3, \ldots$ или $\{a_n\}$. Элемент a_n называется *n-м членом последовательности* $\{a_n\}$.

Заметим, что члены последовательности не обязательно должны быть различными элементами множества M.

Приведём несколько примеров последовательности.

1. Последовательность натуральных чисел $1, 2, 3, \ldots = \{n\}$.

2. $1, \frac{1}{2}, \frac{1}{3}, \ldots = \left\{\frac{1}{n}\right\}$.

3. $1, 0, 1, 0, \ldots = \{a_n\}$,

где a_n есть остаток от деления n на 2.

4. $+1, -2, +3, -4, \ldots = \{n \cdot (-1)^{n+1}\}$.

5. $3, \frac{3}{2}, \frac{7}{3}, \frac{7}{4}, \frac{11}{5}, \frac{11}{6}, \ldots = \left\{2 + \frac{(-1)^{n+1}}{n}\right\}$.

6. $2, 3, 5, 7, \ldots = \{p_n\}$, где p_n — n-е простое число. Здесь мы не можем дать общую формулу для n-го числа p_n. Тем не менее данная последовательность точно определена. Надо лишь воспользоваться индуктивным определением (§ 15, определение 1), положив $f(1)=2$, $f(n)$ есть наименьшее простое число, большее числа $f(n-1)$. Эти условия определяют единственную функцию, заданную на множестве всех натуральных чисел (§ 15, теорема 1). Этот пример показывает, что функция не обязательно должна задаваться некоторой формулой, определяющей её значение через значение аргумента.

Нижеследующие понятия имеют смысл не для любого множества, а лишь для упорядоченного множества или расположенного кольца. Мы ограничимся, однако, только нужным для дальнейшего случаем расположенного поля, содержащего поле рациональных чисел.

Итак, во всём этом параграфе под P следует понимать расположенное поле, содержащее в качестве подполя поле рациональных чисел Г. Всё сказанное в этом параграфе о поле P остаётся справедливым (в силу изоморфизма, установленного в § 23, теорема 2) для любого расположенного поля Q с заменой рациональных чисел r на соответствующие им элементы re, где e — единица поля Q.

Определение 2. *Последовательность* $\{a_n\}$ *элементов поля* P *называется ограниченной сверху* (соответственно *снизу*), *если существует элемент* a *поля* P *такой, что* $a_n < a$ (соответственно $a_n > a$) *для всех* n. *Она называется ограниченной, если она ограничена и сверху и снизу или* (что то же самое) *если существует элемент* $a > 0$ *поля* P *такой, что* $|a_n| < a$ *для всех* n.

Среди приведённых выше примеров последовательность 4 не ограничена ни сверху, ни снизу, а 2, 3, 5 ограничены.

Следующее понятие является одним из основных понятий всей математики.

Определение 3. *Элемент* a *поля* P *называется пределом последовательности* $\{a_n\}$ *элементов* P, *если для любого положительного элемента* ε *из* P *существует* (зависящее от ε) *натуральное число* n_0 *такое, что* $|a_n - a| < \varepsilon$ *для любого* $n > n_0$. Пишут: $a = \lim\limits_{n\to\infty} a_n$ («предел a_n при n, стремящемся к бесконечности») или просто $a = \lim a_n$ («предел a_n»). *Последовательность* $\{a_n\}$, *имеющая предел* a, *называется сходящейся к* a *или просто сходящейся. Последовательность, не имеющая предела* (в P), *называется расходящейся.*

Из приведённых выше последовательностей только две сходятся: последовательность 2 к числу 0 и последовательность 5 к числу 2. В самом деле, для последовательности 2 имеем:

$$|a_n - 0| = |a_n| = a_n = \frac{1}{n};$$

для последовательности 5 также

$$|a_n - 2| = \left|\frac{(-1)^{n+1}}{n}\right| = \frac{1}{n}.$$

Но по аксиоме Архимеда для поля рациональных чисел (§ 23, теорема 3) для любого рационального $\varepsilon > 0$ существует натуральное $n_0 > \frac{1}{\varepsilon}$. Тогда $\frac{1}{n} < \frac{1}{n_0} < \varepsilon$ для любого $n > n_0$.

Последовательность 3 расходится. Правда, для любого $\varepsilon > 0$ и любого n_0 найдётся $n' > n_0$ такое, что $|a_{n'} - 0| = 0 < \varepsilon$ и $n'' > n_0$ такое, что $|a_{n''} - 1| = 0 < \varepsilon$, но для $\varepsilon \leqslant 1$ не существует такого n_0, чтобы одно из указанных неравенств выполнялось для любого $n > n_0$. В самом деле, если, например, $|a_n - 0| = |a_n| < \varepsilon \leqslant 1$, то $a_n = 0$. Следовательно, $a_{n+1} = 1$ и $|a_{n+1} - 0| = 1 \geqslant \varepsilon$.

Понятие предела последовательности сходно с понятием алгебраической операции (§ 6, определение 1). Там упорядоченной паре элементов, а здесь упорядоченной по типу множества натуральных чисел $\{1, 2, 3, \ldots\}$ системе элементов соответствует некоторый элемент того же множества. Поэтому иногда говорят об «операции

предельного перехода». Разумеется, это уже не алгебраическая операция в смысле определения 1 из § 6.

Возникает вопрос о выполнимости и однозначности операции предельного перехода. Что не всякая последовательность имеет предел, мы уже видели на примере последовательности 3. Вопрос об единственности предела решается утвердительно. Именно:

Теорема 1. *Если последовательность элементов поля P имеет предел, то только один.*

Доказательство. Пусть $\lim a_n = a$ и $b \neq a$. Покажем, что b уже не будет пределом нашей последовательности. Наглядное представление говорит, что элементы a_n, приближаясь к a, отойдут для больших номеров от b. Формально это доказывается так. Так как $a \neq b$, то $|a-b| > 0$ и $\frac{|a-b|}{2} > 0$. Если также $\lim a_n = b$, то существуют натуральные числа n_1 и n_2 такие, что $|a_n - a| < \frac{|a-b|}{2}$ при любом $n > n_1$ и $|a_n - b| < \frac{|a-b|}{2}$ при любом $n > n_2$.

Если n_0 — большее из чисел n_1 и n_2, то при $n > n_0$ получим:

$$|a-b| = |(a-a_n)+(a_n-b)| \leqslant |a-a_n| + |a_n-b| < \\ < \frac{|a-b|}{2} + \frac{|a-b|}{2} = |a-b|,$$

т. е. $|a-b| < |a-b|$, что невозможно.

Отложив пока вопрос об условиях существования предела, найдём некоторые свойства операции предельного перехода в случае её выполнимости.

Теорема 2. а) *Если одна из последовательностей $\{a_n\}$ и $\{b_n\}$ элементов поля P сходится и если $\lim (a_n - b_n) = 0$, то и другая последовательность сходится, причём $\lim a_n = \lim b_n$.*

Обратно, *если обе последовательности сходятся и если $\lim a_n = \lim b_n$, то $\lim (a_n - b_n) = 0$.*

Далее, *если последовательности $\{a_n\}$ и $\{b_n\}$ из P сходятся, то*

б) $\lim (a_n \pm b_n) = \lim a_n \pm \lim b_n$;

в) $\lim (a_n \cdot b_n) = \lim a_n \cdot \lim b_n$;

г) $\lim \frac{a_n}{b_n} = \frac{\lim a_n}{\lim b_n}$

при условии, что $\lim b_n \neq 0$ и $b_n \neq 0$ при любом n.

Сходимость последовательностей в левых частях равенств б), в), г) *не предполагается, а следует из сходимости последовательностей $\{a_n\}$ и $\{b_n\}$.*

д) *Если $\lim a_n > \lim b_n$, то существует элемент $\varepsilon > 0$ из P и натуральное число n_0 такие, что $a_n - b_n > \varepsilon$ при любом $n > n_0$. Если существует натуральное число n_0 такое, что $a_n \geqslant b_n$ при любом $n > n_0$, то $\lim a_n \geqslant \lim b_n$.*

Доказательство. а) Пусть, например, последовательность $\{a_n\}$ сходится, причём $\lim a_n = a$. Тогда для любого $\varepsilon > 0$ из P существуют натуральные числа $n_1 < n_2$ такие, что $|a_n - a| < \frac{\varepsilon}{2}$ при любом $n > n_1$ и $|a_n - b_n| < \frac{\varepsilon}{2}$ при любом $n > n_2$. Если n_0 — большее из чисел n_1 и n_2, то

$$|b_n - a| = |(b_n - a_n) + (a_n - a)| \leqslant |b_n - a_n| + |a_n - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Таким образом,

$$\lim b_n = a = \lim a_n.$$

Второе утверждение пункта а) следует из пункта б).

Пусть теперь последовательности $\{a_n\}$ и $\{b_n\}$ сходятся, причём $\lim a_n = a$ и $\lim b_n = b$.

б) Для любого $\varepsilon > 0$ существуют натуральные числа n_1 и n_2 такие, что $|a_n - a| < \frac{\varepsilon}{2}$ при любом $n > n_1$ и $|b_n - b| < \frac{\varepsilon}{2}$ при любом $n > n_2$. Если n_0 — большее из чисел n_1 и n_2, то при любом $n > n_0$ будет:

$$|(a_n \pm b_n) - (a \pm b)| = |(a_n - a) \pm (b_n - b)| \leqslant$$
$$\leqslant |a_n - a| + |b_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Таким образом,

$$\lim (a_n \pm b_n) = a \pm b = \lim a_n \pm \lim b_n.$$

в) Сначала покажем, что сходящаяся последовательность $\{a_n\}$ ограничена (см. определение 2). Так как $\lim a_n = a$, то существует p такое, что $|a_n - a| < 1$ при любом $n > p$. Тогда

$$|a_n| = |(a_n - a) + a| \leqslant |a_n - a| + |a| < 1 + |a|$$

при $n > p$. Среди конечной совокупности элементов $|a_1|, |a_2|, \ldots$ $\ldots, |a_p|, 1 + |a|$ поля P существует наибольший элемент a' (§ 5, теорема 6). Если положим $c = a' + 1$, то $c \geqslant 1 > 0$ и $|a_n| < c$ для всех n.

Далее, берём любой элемент $d > |b|$, например $d = |b| + 1$. Тогда, очевидно, $d > 0$. Так как $\lim a_n = a$ и $\lim b_n = b$, то для любого $\varepsilon > 0$ из P существуют натуральные числа n_1 и n_2 такие, что $|a_n - a| < \frac{\varepsilon}{2d}$ при любом $n > n_1$ и $|b_n - b| < \frac{\varepsilon}{2c}$ при любом $n > n_2$. Если n_0 — большее из чисел n_1 и n_2, то

$$|a_n b_n - ab| = |(a_n b_n - a_n b) + (a_n b - ab)| \leqslant$$
$$\leqslant |a_n b_n - a_n b| + |a_n b - ab| = |a_n| \cdot |b_n - b| + |a_n - a| \cdot |b| <$$
$$< c \cdot \frac{\varepsilon}{2c} + \frac{\varepsilon}{2d} \cdot d = \varepsilon$$

при любом $n > n_0$. Таким образом,

$$\lim (a_n b_n) = ab = \lim a_n \cdot \lim b_n.$$

г) Сначала докажем, что при условии $\lim b_n = b \neq 0$ существует натуральное число n_1 такое, что $|b_n| > \frac{|b|}{2}$ при любом $n > n_1$. Существует натуральное число p такое, что $|b_n - b| < \frac{|b|}{2}$ при любом $n > p$. Если бы доказываемое утверждение было неверно, то для числа p нашлось бы число $q > p$ такое, что $|b_q| < \frac{|b|}{2}$. Тогда

$$|b| = |(b - b_q) + b_q| \leqslant |b - b_q| + |b_q| < \frac{|b|}{2} + \frac{|b|}{2} = |b|,$$

т. е. $|b| < |b|$, что невозможно. Последовательность $\{a_n\}$ сходится, а потому ограничена, т. е. существует элемент $c > 0$ из P такой, что $|a_n| < c$ при любом n.

Наконец, из $\lim a_n = a$ и $\lim b_n = b$ следует, что для любого $\varepsilon > 0$ из P существуют натуральные числа n_2 и n_3 такие, что $|a_n - a| < \frac{\varepsilon \cdot |b|}{2}$ при любом $n > n_2$ и $|b_n - b| < \frac{\varepsilon \cdot b^2}{4c}$ при любом $n > n_3$ (ибо для $b \neq 0$ всегда $b^2 = |b|^2 > 0$). Пусть n_0 — наибольшее из чисел n_1, n_2 и n_3. Тогда

$$\left|\frac{a_n}{b_n} - \frac{a}{b}\right| = \left|\frac{a_n b - b_n a}{b_n b}\right| = \frac{|(a_n b - a_n b_n) + (a_n b_n - b_n a)|}{|b_n b|} \leqslant \frac{|a_n b - a_n b_n|}{|b_n b|} +$$

$$+ \frac{|a_n b_n - b_n a|}{|b_n b|} = \frac{|a_n|\,|b - b_n|}{|b|\,|b_n|} + \frac{|a_n - a|}{|b|} < \frac{c \cdot \frac{\varepsilon b^2}{4c}}{\frac{|b|}{2}|b|} + \frac{\frac{\varepsilon |b|}{2}}{|b|} = \varepsilon$$

при любом $n > n_0$. Таким образом,

$$\lim \frac{a_n}{b_n} = \frac{a}{b} = \frac{\lim a_n}{\lim b_n}.$$

д) Пусть $a > b$. Берём $\varepsilon = \frac{a - b}{3} > 0$. Существуют натуральные числа n_1 и n_2 такие, что $|a_n - a| < \varepsilon$ при любом $n > n_1$ и $|b_n - b| < \varepsilon$ при любом $n > n_2$. Пусть n_0 — большее из чисел n_1 и n_2. Если при некотором $n > n_0$ будет $a_n - b_n \leqslant \varepsilon$, то для такого n найдём:

$$a - b = (a - a_n) + (a_n - b) + (b_n - b) < \varepsilon + \varepsilon + \varepsilon = 3\varepsilon = a - b,$$

что невозможно. Стало быть, $a_n - b_n > \varepsilon$ при любом $n > n_0$. Пусть, обратно, $a_n - b_n \geqslant 0$ при любом $n > n_0$. Если бы было $a < b$, то по доказанному существовали бы $\varepsilon > 0$ и n_1 такие, что $b_n - a_n > \varepsilon > 0$ при любом $n > n_1$. Беря любое n больше как n_0, так и n_1, получим: $a_n \geqslant b_n$ и $b_n > a_n$, что невозможно. Следовательно, $a \geqslant b$. Теорема доказана.

Если последовательность имеет предел, то её члены, приближаясь к этому пределу, должны сближаться между собой по мере роста их номеров. Дадим точное определение этого свойства последовательности.

Определение 4. *Последовательность $\{a_n\}$ элементов поля P называется фундаментальной* (или *последовательностью Коши*), *если для любого элемента $\varepsilon > 0$ из P существует натуральное число n_0* (зависящее от ε) *такое, что $|a_p - a_q| < \varepsilon$ для любых p и q, бо́льших n_0.*

Теорема 3. *Всякая сходящаяся последовательность элементов поля P является фундаментальной.*

Доказательство. Пусть $\lim a_n = a$. Для любого $\varepsilon > 0$ из P существует натуральное число n_0 такое, что $|a_n - a| < \frac{\varepsilon}{2}$ при любом $n > n_0$. Если тогда $p > n_0$ и $q > n_0$, то по свойству абсолютных величин [§ 10, (3)] найдём:

$$|a_p - a_q| = |(a_p - a) - (a_q - a)| \leqslant |a_p - a| + |a_q - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

т. е. последовательность $\{a_n\}$ — фундаментальная.

Эта теорема даёт необходимый признак сходимости последовательности: для того чтобы последовательность была сходящейся, необходимо, чтобы она была фундаментальной. Однако это условие не для любого поля P является достаточным. Так, в поле рациональных чисел, как мы сейчас увидим, существуют фундаментальные последовательности, не имеющие (в этом поле) предела.

Вернёмся ещё к задачам об отношении отрезков и извлечении корня. Для каждой из них мы построили две последовательности рациональных (даже десятично-рациональных) чисел a_n и b_n со свойствами (1). Легко видеть, что каждая из них будет фундаментальной. Для любого рационального ε существует натуральное n_0 такое, что $\frac{1}{10^{n_0}} < \varepsilon$ (§ 23, теорема 5). Тогда для любых p и q, где, например, $p \geqslant q > n_0$, получим:

$$|a_p - a_q| = a_p - a_q < b_p - a_q \leqslant b_{n_0} - a_{n_0} = \frac{1}{10^{n_0}} < \varepsilon$$

и аналогично этому $|b_p - b_q| < \varepsilon$.

Если данная задача имеет решением рациональное число c, то c должно быть пределом обеих последовательностей $\{a_n\}$ и $\{b_n\}$. В самом деле, в случае отрезков $c \cdot AB = MN < b_n \cdot AB$, откуда $c < b_n$. Также $a_n \cdot AB \leqslant MN = c \cdot AB$, откуда $a_n \leqslant c$. В случае корней $c^k = a$, откуда $a_n \leqslant c < b_n$, так как из $a_n > c$ следует $a_n^k > c^k = a$ и из $b_n \leqslant c$ следует $b_n^k \leqslant c^k = a$, что противоречит построению

чисел a_n и b_n. Но из $a_n \leqslant c < b_n$ следует, что для любого $\varepsilon > 0$ существует n_0 такое, что $\frac{1}{10^{n_0}} < \varepsilon$, и тогда при $n > n_0$ будет:

$$|a_n - c| = c - a_n < b_n - a_n \leqslant b_{n_0} - a_{n_0} = \frac{1}{10^{n_0}} < \varepsilon,$$

и аналогично $|b_n - c| < \varepsilon$, т. е.

$$\lim a_n = \lim b_n = c.$$

Итак, каждый раз, как задача имеет решение, она решается предельным переходом.

Обратно, если, например, последовательность $\{a_n\}$ имеет рациональный предел c, то и $\lim b_n = c$, причём число c решает данную задачу. В самом деле, из $\lim a_n = c$ следует $a_n \leqslant c \leqslant b_n$ для любого n. Иначе при некотором n_1 будет $a_{n_1} > c$ и при любом $n > n_1$ имеем:

$$a_n > a_{n_1} > c, \quad |a_n - c| = a_n - c \geqslant a_{n_1} - c,$$

или же при некотором n_2 будет $b_{n_2} < c$ и при любом $n > n_2$ имеем:

$$a_n < b_n \leqslant b_{n_2} < c, \quad |a_n - c| = c - a_n > c - b_{n_2},$$

что противоречит определению предела. Но из $a_n \leqslant c \leqslant b_n$, как выше мы видели, следует $\lim a_n = \lim b_n = c$.

То, что число c решает поставленную задачу, будет для извлечения корня следовать из более общей теоремы и притом сразу для всех действительных чисел. Здесь мы докажем, что если построенные в начале параграфа для рационального числа $a > 0$ и натурального числа $k > 1$ последовательности рациональных чисел $\{a_n\}$ и $\{b_n\}$ имеют рациональный предел c, то $c^k = a$. Предположим, что $c^k < a$. Так как $\lim b_n = c$, то по теореме 2, в) также $\lim b_n^k = c^k$. Следовательно, существует натуральное число n_0 такое, что $|b_n^k - c^k| < a - c^k$ при любом $n > n_0$. Но из $b_n \geqslant c \geqslant a_n \geqslant 0$ следует $b_n^k \geqslant c^k$. Поэтому

$$|b_n^k - c^k| = b_n^k - c^k < a - c^k,$$

откуда $b_n^k < a$, что противоречит построению числа b_n. Так же доказывается, что не имеет места неравенство $c^k > a$. Таким образом, $c^k = a$, $c = \sqrt[k]{a}$.

Если рациональное число $a > 0$ таково, что не существует рационального числа c, для которого $c^k = a$ (см. конец § 23), то последовательности $\{a_n\}$ и $\{b_n\}$, построенные для этих a и k, не имеют предела в поле рациональных чисел, хотя являются фундаментальными.

В случае отношения отрезков надо доказать, что если построенные для отрезков AB и MN последовательности рациональных чисел $\{a_n\}$ и $\{b_n\}$ сходятся к рациональному числу c, то c и будет отношением этих отрезков, т. е. $c \cdot AB = MN$. Пусть это не так,

тогда, например, $c \cdot AB < MN$, или $c \cdot AB = MN_1$, причём отрезок MN_1 составляет часть отрезка MN. Как бы мал ни был отрезок N_1N, по геометрической аксиоме Архимеда найдётся натуральное k такое, что $k \cdot N_1N > AB$. Но $10^k > k$ [§ 23, (3)] и $10^k \cdot N_1N > AB$, откуда $\frac{AB}{10^k} < N_1N$. Число a_k определялось так, что

$$a_k \cdot AB \leqslant MN < b_k \cdot AB,$$

где

$$b_k - a_k = \frac{1}{10^k}.$$

Но из $a_k \leqslant c$ следует, что

$$b_k \cdot AB = a_k \cdot AB + (b_k - a_k) \cdot AB \leqslant c \cdot AB + \frac{AB}{10^k} < \\ < MN_1 + N_1N = MN,$$

что невозможно ввиду $b_k \cdot AB > MN$. Также придём к противоречию, предположив, что $c \cdot AB > MN$. Таким образом $c \cdot AB = MN$.

Если отрезки AB и MN несоизмеримы, то их отношение не может выражаться рациональным числом, а потому построенные для отрезков последовательности рациональных чисел $\{a_n\}$ и $\{b_n\}$ не имеют предела в поле рациональных чисел, хотя и являются фундаментальными.

Итак, *в поле рациональных чисел существуют фундаментальные последовательности, не имеющие предела.*

Определение 5. *Расположенное поле называется полным, если оно обладает следующим свойством:*

XII (аксиома полноты). *Любая фундаментальная последовательность элементов данного поля сходится, т. е. имеет предел в этом поле.*

Из сказанного выше вытекает

Теорема 4. *Поле рациональных чисел* Г *не является полным.*

Мы дали выше два доказательства этой теоремы, построив расходящиеся фундаментальные последовательности рациональных чисел для несоизмеримых отрезков и для рационального числа, не являющегося k-й степенью никакого рационального числа. Доказательство с помощью отрезков опиралось на положения геометрии, которые здесь не обосновывались. Другое же доказательство опиралось лишь на доказанные нами свойства рациональных чисел и потому может считаться доведённым до конца.

Замечание. Введённые выше понятия фундаментальной последовательности, её предела и связанное с ними понятие полного поля имеют одно свойство, коренным образом отличающее их от введённых ранее понятий: алгебраических операций, расположения и архимедовского расположения. Именно, пусть дано поле P и его подполе P'. Если для элементов a, b, c из подполя P' имеет место соотношение $a + b = c$, то это соотношение по самому определе-

нию подполя (§ 8, определение 3) сохраняется и в поле P. Обратно, если $a+b=c$ в P, причём элементы a, b, c входят в P', то и в P' будет $a+b=c$. То же верно для отношения $ab=c$. Если поле P расположено, то этим порождается расположение P'. Именно, считаем $a>0$ в P' тогда и только тогда, когда $a>0$ в P. Легко видеть, что свойства расположения IX и X (§ 10, определение 1) будут в P' выполнены, т. е. P' будет расположенным полем. Такое свойство расположения P' быть архимедовским не зависит от того, рассматриваем ли мы P' само по себе или как подполе поля P. В самом деле, отношение $ne>a$ для элементов e и a из P' тогда и только тогда имеет место в P', когда оно имеет место в P (при условии совпадения порядка). В этом смысле понятия, введённые в главе II, являются абсолютными. Они не зависят от объемлющего поля. Понятия же данного параграфа, указанные выше, зависят от поля, в котором данные элементы рассматриваются, и в этом смысле эти понятия относительны. Так, отношение $\lim a_n=a$ означает, что для любого элемента $\varepsilon>0$ из поля P существует натуральное число n_0 такое, что $|a_n-a|<\varepsilon$ при любом $n>n_0$. Определение фундаментальной последовательности также содержит упоминание любого элемента $\varepsilon>0$ поля P. Но запас этих элементов ε зависит от выбора поля P', и нет основания ожидать, что если все эти элементы последовательности $\{a_n\}$ и a входят в подполе P' поля P, то смысл отношения $\lim a_n=a$ и свойство фундаментальности последовательности $\{a_n\}$ в P и в P' будут совпадать. Ясно лишь, что из выполнения одного из условий в P следует его выполнение в P', ибо то, что верно для любого $\varepsilon>0$ из P и для данных элементов из P', останется верным, в частности, и для любого $\varepsilon>0$ из P'; но обратного заключить нельзя. Покажем на примере, что это действительно так.

Пусть P — поле рациональных функций (т. е. алгебраических дробей) $\frac{f(x)}{g(x)}$, где $f(x)$ и $g(x)$ — многочлены с рациональными коэффициентами. Считая функцию $\frac{f(x)}{g(x)}$ положительной, если старшие коэффициенты многочленов $f(x)$ и $g(x)$ имеют одинаковые знаки, получим расположение поля P. Оно не будет архимедовским, так как при любом натуральном n будет $x-n=\frac{x-n}{1}>0$, откуда $n\cdot 1<x$. Итак, x больше всех рациональных чисел. Если $a>0$ рационально, то и $a^{-1}>0$ рационально и $a^{-1}<x$. Умножая на $\frac{a}{x}>0$, найдём $\frac{1}{x}<a$. Итак, $\frac{1}{x}$ меньше всех положительных рациональных чисел. Поле P содержит подполе Γ рациональных чисел. В Γ последовательность $\left\{\frac{1}{n}\right\}$, $n=1, 2, 3, \ldots$, сходится к числу 0 и, следовательно, фундаментальна, но в поле P будет $\left|\frac{1}{n}\right|=\frac{1}{n}>\frac{1}{x}$ при любом n, и 0 уже не будет пределом этой последовательности.

В P она вообще не может иметь предела, так как не будет фундаментальной. В самом деле, при $p \neq q$ число

$$\left|\frac{1}{p}-\frac{1}{q}\right|>0$$

и рационально. Таким образом $\left|\frac{1}{p}-\frac{1}{q}\right|>\frac{1}{x}$. Легко видеть, что в поле P последовательность рациональных чисел $\{a_n\}$ фундаментальна тогда и только тогда, когда она становится стационарной, т. е. существует рациональное a и n_0 такие, что $a_n=a$ при любом $n>n_0$. Тогда, очевидно, $\lim a_n=a$. Таким образом, перенося операцию предельного перехода с поля P на подполе Γ, мы получим полное поле, хотя Γ неполно в смысле данного выше определения 5.

Тем не менее в одном случае введённые в этом параграфе понятия остаются абсолютными. Именно:

Теорема 5. *Для того чтобы понятия предела и фундаментальной последовательности в поле P совпадали с теми же понятиями в любом его подполе P', необходимо и достаточно, чтобы расположение поля P было архимедовским* [1]).

Доказательство. Если поле P расположено неархимедовски, то существует элемент c такой, что $n<c$ для любого натурального n. Так как поле рациональных чисел Γ архимедовски расположено, то $a<c$ для любого рационального a. Тогда при $a>0$ и рациональном, умножая $a<c$ на $\frac{1}{ac}>0$, найдём $\frac{1}{c}<\frac{1}{a}$, т. е. $0<\frac{1}{c}<b$, где $b=\frac{1}{a}$ — любое рациональное положительное число. Очевидно, последовательность $\left\{\frac{1}{n}\right\}$, $n=1, 2, 3, \ldots$, рациональных чисел в поле Γ сходится к числу 0 и потому фундаментальна. Но та же последовательность в поле P не является фундаментальной и потому не имеет предела. В самом деле, берём: $\varepsilon=\frac{1}{c}>0$. Тогда при $p \neq q$ будет: $\left|\frac{1}{p}-\frac{1}{q}\right|>\varepsilon$. Стало быть не существует числа n_0 со свойством $\left|\frac{1}{p}-\frac{1}{q}\right|<\varepsilon$ при любых p и q, бо́льших n_0. Необходимость доказана.

Пусть теперь поле P архимедовски расположено. Покажем независимость свойства последовательности $\{a_n\}$ быть сходящейся или

---

[1]) Из доказательства этой теоремы следует, что архимедовость расположения поля P необходима даже для того, чтобы понятия предела и фундаментальной последовательности совпадали в поле P и содержащемся в нём поле рациональных чисел Γ. Другими словами, если фундаментальные и сходящиеся последовательности в поле Γ остаются такими же и в поле P, то поле P архимедовски расположено. Этим мы воспользуемся в начале следующего параграфа.

фундаментальной от подполя P', содержащего элементы a_n и (для случая сходимости) предел $a=\lim a_n$. Из выполнения этих свойств в P следует их выполнение в P'. Пусть, например, $\lim a_n=a$ в P'. Покажем, что то же будет и в P. Берём любой элемент $\varepsilon>0$ из P. Так как P архимедовски расположено, то существует натуральное $n>\frac{1}{\varepsilon}$, откуда $0<\frac{1}{n}=\varepsilon'<\varepsilon$. Число $\varepsilon'>0$ входит в любое подполе поля P, а следовательно, и в P'. Так как в P' дано $\lim a_n=a$, то существует натуральное n_0 такое, что $|a_n-a|<\varepsilon'<\varepsilon$ при любом $n>n_0$. Это означает, что $\lim a_n=a$ также и в поле P. Теорема доказана.

Определение 6. *Полное, архимедовски расположенное поле называется непрерывным.*

В непрерывном поле задачи об отношении отрезков и извлечении корня из положительного элемента всегда разрешимы. К задаче об извлечении корня мы ещё вернёмся в § 26. Скажем несколько слов об отношении отрезков. Если бы нам удалось расширить поле рациональных чисел Г до непрерывного поля P, то по последней теореме последовательности рациональных чисел $\{a_n\}$ и $\{b_n\}$, построенные выше для данных отрезков AB и MN, были бы фундаментальными не только в Г, но и в P. Так как поле P полно, то они имели бы общий предел c [теорема 2, а)]. Элемент c по определению можно принять за отношение данных отрезков, т. е. считать, что $MN:AB=c$ или $MN=c\cdot AB$. Это новое определение отношения в случае соизмеримых отрезков согласуется, как выше показано, с прежним определением (см. конец § 23). Но, в то время как прежнее определение годилось лишь для соизмеримых отрезков, новое определение даёт определённый элемент поля P для любых отрезков независимо от их соизмеримости. В этом смысле задача об отношении отрезков разрешима в непрерывном поле P. Мы рассмотрели эту задачу лишь для иллюстрации важности понятия непрерывного поля и не можем остановиться на этой геометрической задаче подробнее.

Заметим уже без доказательства, что определённое выше отношение отрезков обладает всеми нужными свойствами. Именно, для любых отрезков AB и CD и любых элементов $c>0$ и $d>0$ непрерывного поля P будет:

а) из $c<d$ следует: $c\cdot AB<d\cdot AB$;

б) $(c+d)\,AB=c\cdot AB+d\cdot AB$;

в) $c(AB+CD)=c\cdot AB+c\cdot CD$.

Далее, для любого отрезка AB и любого элемента $c>0$ из P существует отрезок MN такой, что $MN:AB=c$.

К задаче о длине отрезка сводится задача о длине окружности. Мы строим две последовательности правильных многоугольников (вписанных и описанных) путём удвоения числа сторон. Зная

отношение отрезков, мы можем найти периметры a_n и b_n n-го вписанного и n-го описанного многоугольника. Известными из школы рассуждениями можно показать, что $a_1 < a_2 < \dots$ и $b_1 > b_2 > \dots$ Далее $a_n < b_n$ и $\lim (b_n - a_n) = 0$.

Отсюда легко вывести, что обе последовательности, $\{a_n\}$ и $\{b_n\}$, элементов поля P фундаментальны и в силу полноты P имеют в нём общий предел c. Элемент c поля P по определению принимается за длину окружности. Аналогично определяется длина дуги данной окружности. Можно показать, что длина дуги заключена между нулём и длиной окружности c и, обратно, для каждого элемента c' поля P такого, что $0 < c' < c$, можно найти дугу данной окружности длины c'. В этом смысле задача о длине дуги окружности также решается в непрерывном поле P.

В следующем параграфе мы увидим, что непрерывное поле и будет полем действительных чисел.

§ 25. Определение поля действительных чисел

В поле рациональных чисел Г не всегда выполнима операция предельного перехода для фундаментальной последовательности, т. е. поле Г не является полным (§ 24, теорема 4). Следуя общему плану расширения числовых совокупностей, намеченному в § 18, мы расширим поле Г до нового поля D, в котором было бы определено расположение и любая фундаментальная последовательность имела бы предел. При этом мы хотим, чтобы операция предельного перехода, не всегда выполнимая в Г для фундаментальных последовательностей, в новом поле D для тех же последовательностей из Г была уже выполнима. Стало быть, фундаментальные последовательности из Г должны оставаться фундаментальными и в D. Это означает, что D должно быть полным и архимедовски расположенным полем (§ 24, теорема 5). Иными словами, D должно быть непрерывным полем. Как и в случае целых (§ 20) и рациональных (§ 22) чисел, мы ищем минимальное расширение с нужными свойствами. Однако оказывается, что условие минимальности будет выполнено само собой, так как требование непрерывности определяет поле однозначно с точностью до изоморфизма. Поэтому было бы излишним включать в определение требование минимальности. Так, мы приходим к определению:

Определение 1. *Полем действительных чисел называется непрерывное поле D, содержащее в качестве подполя поле рациональных чисел* Г. *Элементы поля D называются действительными числами.*

Доказательство существования и единственности поля D, удовлетворяющее этому определению, проходит аналогично случаю кольца целых чисел (§ 20) и поля рациональных чисел (§ 22). Начнём с доказательства единственности.

Теорема 1. *Расположенное поле P, содержащее поле рациональных чисел* Γ [1]), *архимедовски расположено тогда и только тогда, когда каждый элемент поля P равен пределу последовательности рациональных чисел.*

Доказательство. а) Пусть элемент a поля P равен пределу последовательности рациональных чисел $\{a_n\}$. Тогда существует k такое, что $|a_k - a| < 1$, откуда

$$a \leqslant |a| = |(a - a_k) + a_k| \leqslant |a - a_k| + |a_k| < 1 + |a_k|.$$

Так как $1 + |a_k|$ — рациональное число и поле рациональных чисел архимедовски расположено, то существует натуральное число n такое, что $1 + |a_k| < n$. Тогда $a < n$, т. е. поле P архимедовски расположено (§ 10, XI').

б) Пусть поле P архимедовски расположено. Тогда для любого элемента a из P и любого натурального числа n существуют натуральные числа m_1 и m_2 такие, что

$$m_1 \cdot \frac{1}{n} > a \text{ и } m_2 \cdot \frac{1}{n} > -a,$$

откуда $(-m_2) \cdot \frac{1}{n} < a$. Следовательно множество A тех целых чисел l, для которых $l \cdot \frac{1}{n} \leqslant a$, ограничено сверху числом m_1 и непусто, ибо содержит целое число $-m_2$. Поэтому множество A содержит наибольшее число m (§ 21, теорема 5). Тогда, очевидно, $\frac{m}{n} \leqslant a < \frac{m+1}{n}$. Вычтя $\frac{m}{n}$ из обеих частей неравенства, найдём: $0 \leqslant a - \frac{m}{n} < \frac{1}{n}$. Положим $\frac{m}{n} = a_n$ и покажем, что $\lim a_n = a$. Для любого $\varepsilon > 0$ из P существует натуральное $n_0 > \frac{1}{\varepsilon}$, откуда

$$|a_n - a| = a - a_n < \frac{1}{n} < \frac{1}{n_0} < \varepsilon$$

при любом $n > n_0$. Это и значит, что $\lim a_n = a$ в поле P.

Теорема 2. *Все поля действительных чисел изоморфны, т. е. поле действительных чисел определено однозначно до изоморфизма. Точнее, если D_1 и D_2 — два поля действительных чисел, то существует только одно изоморфное отображение D_1 на D_2, сохраняющее отношения порядка. При этом изоморфизме рациональные числа остаются на месте. В частности, существует только одно изоморфное отображение поля действительных чисел на себя, сохраняющее отношения порядка, а именно тождественное.* (В силу теоремы 2 из § 23 данная теорема остаётся справедливой

[1]) Условие $P \supset \Gamma$ можно здесь и ниже опустить, заменив рациональные числа на рациональные элементы поля (§ 22, теорема 2).

для любых непрерывных полей с заменой рациональных чисел рациональными элементами [1]).

Доказательство. Строим отображение f поля D_1 в поле D_2 следующим образом. Пусть d_1 — любой элемент поля D_1. Так как D_1 архимедовски расположено, то по теореме 1 $d_1 = \lim a_n$ с рациональными a_n. Таким образом, последовательность $\{a_n\}$ фундаментальна в D_1, а потому и в его подполе Г. Так как $\Gamma \subset D_2$ и D_2 архимедовски расположено, то последовательность $\{a_n\}$, фундаментальная в Г, будет фундаментальной и в D_2 (§ 24, теорема 5). Так как D_2 полно, то $\lim a_n = d_2$ в D_2. Мы положим $f(d_1) = d_2$.

Покажем, что элемент d_2 не зависит от выбора последовательности рациональных чисел $\{a_n\}$. Если ещё $\lim b_n = d_1$ с рациональными b_n, то $\lim a_n = \lim b_n$, откуда $\lim (a_n - b_n) = 0$ [§ 24, теорема 2, а)] в D_1, а следовательно, в Г. Рассуждая, как выше, мы найдём, что $\lim (a_n - b_n) = 0$ в D_2 и $\lim a_n = \lim b_n = d_2$. Если d_1 — рациональное число, то $\lim a_n = d_1$, где $a_n = d_1$ при любом n. Таким образом, $f(d_1) = d_1$, т. е. отображение f оставляет на месте рациональные числа.

Если $c_1 \neq d_1$ и $c_1 = \lim a_n$, $d_1 = \lim b_n$, то $\lim (a_n - b_n) \neq 0$ и $\lim a_n \neq \lim b_n$ в D_2, т. е. $f(c_1) \neq f(d_1)$. Итак, отображение f является взаимно однозначным отображением D_1 в D_2. Оно зависит от определения предела в D_1 и D_2, а потому зависит от отношений порядка в этих полях.

Покажем, что f есть изоморфное отображение D_1 в D_2. Надо показать, что для любых элементов c_1 и d_1 из D_1 будет:

$$f(c_1 + d_1) = f(c_1) + f(d_1), \quad f(c_1 d_1) = f(c_1) f(d_1).$$

Это легко следует из теоремы 2, б), в) § 24, именно, если $c_1 = \lim a_n$, $d_1 = \lim b_n$, то, применяя определение отображения f, имеем:

$$\begin{aligned} f(c_1 + d_1) &= f(\lim a_n + \lim b_n) = f[(\lim (a_n + b_n)] = \\ &= \lim f(a_n + b_n) = \lim [f(a_n) + f(b_n)] = \\ &= \lim f(a_n) + \lim f(b_n) = f(\lim a_n) + f(\lim b_n) = \\ &= f(c_1) + f(d_1), \end{aligned}$$

и аналогично доказывается второе равенство.

Покажем, что отображение f сохраняет отношение порядка. Пусть $c_1 < d_1$ в поле D_1 и $c_1 = \lim a_n$, $d_1 = \lim b_n$. Тогда существует n_0 такое, что $a_n < b_n$ при любом $n > n_0$ [§ 24, теорема 2, д)] и $\lim a_n \leqslant \lim b_n$ в D_2, т. е. $f(c_1) \leqslant f(d_1)$.

Но из $c_1 \neq d_1$ следует: $f(c_1) \neq f(d_1)$. Таким образом, $f(c_1) < f(d_1)$.

Покажем, что f является единственным изоморфным отображением D_1 в D_2, сохраняющим отношения порядка. Пусть g — другое

[1]) В § 26 мы увидим, что ограничение изоморфизмами, сохраняющими отношения порядка, можно отбросить, так как поле действительных чисел допускает единственное расположение.

отображение такого рода. При изоморфизме g поле рациональных чисел Г, содержащееся в D_1, отобразится изоморфно на поле рациональных элементов поля D_2, причём рациональное число r перейдёт в элемент re, где e — единица поля D_2 [§ 23, теорема 2]. Но D_2 содержит Г, т. е. $e=1$, $re=r\cdot 1=r$. Следовательно, $g(r)=r$ для любого рационального r. Так как отображение g отлично от f, то существует элемент d_1 из D_1 такой, что $a_2=f(d_1)\neq g(d_1)=b_2$. Найдём рациональное число c, лежащее между a_2 и b_2. Пусть, например, $a_2<b_2$. Рассуждая, как и в доказательстве теоремы 1, пункт б), найдём сначала натуральное n такое, что $\frac{1}{n}<b_2-a_2$, а затем целое число m такое, что $\frac{m}{n}\leqslant a_2<\frac{m+1}{n}$. Если $c=\frac{m+1}{n}$, то получим:

$$a_2<c=\frac{m}{n}+\frac{1}{n}<a_2+(b_2-a_2)=b_2.$$

Так как $c=f(c)$ и f по доказанному сохраняет отношения порядка, то из $f(d_1)=a_2<c$ следует: $d_1<c$. Так как $g(c)=c$ и g также сохраняет порядок, то

$$g(d_1)=b_2<g(c)=c,$$

что противоречит построению числа c.

До сих пор мы не использовали полноты поля D_1. Стало быть, всё доказанное выше верно для любого архимедовски расположенного поля D_1. Нам осталось доказать, что построенное отображение f является отображением поля D_1 на всё поле D_2. Для этого нужна полнота поля D_1. Надо для любого элемента d_2 из D_2 найти элемент d_1 из D_1 такой, что $f(d_1)=d_2$. Так как D_2 архимедовски расположено, то по теореме 1 $d_2=\lim a_n$ с рациональными a_n. Последовательность $\{a_n\}$, фундаментальная в D_2, будет фундаментальной в $\Gamma\subset D_2$, а следовательно, и в поле $D_1\subset\Gamma$. Так как D_1 полно, то существует $d_1=\lim a_n$ в D_1. По определению f тогда $f(d_1)=d_2$. Теорема доказана.

Теорема 3. *Любое архимедовски расположенное поле P изоморфно некоторому подполю поля действительных чисел D. Существует лишь одно изоморфное отображение P в D, сохраняющее отношения порядка. В частности, поле P только одним способом, а именно тождественно, может быть изоморфно и с сохранением порядка отображено само на себя*[1]).

---

[1]) В отличие от теоремы 2 условие о сохранении порядка здесь опустить нельзя. В самом деле, пусть P — поле всех чисел вида $a+b\sqrt{2}$ с рациональными a и b. Отображение $a+b\sqrt{2}\longleftrightarrow a-b\sqrt{2}$ изоморфно относительно сложения и умножения и отлично от тождественного. Но оно не сохраняет порядка, заданного в поле P, как подполе поля действительных чисел, ибо $1+\sqrt{2}>0$, а $1+\sqrt{2}\longleftrightarrow 1-\sqrt{2}<0$.

Доказательство. Поле P изоморфно и с сохранением порядка отображается на расположенное поле Q, содержащее поле рациональных чисел. Так как P архимедовски расположено, то то же верно для Q. Для поля Q теорема получается попутно при доказательстве теоремы 2, если заменить там D_1 на Q, так как везде, кроме последнего абзаца доказательства, мы не пользовались полнотой поля D_1. В силу изоморфизма P и Q теорема 3 верна также для поля P.

Итак, если поле действительных чисел D существует, то только одно (до изоморфизма).

Переходим к доказательству его существования. Как и в случае целых и рациональных чисел, достаточно построить одно поле (одну интерпретацию поля), удовлетворяющее определению 1.

Существует несколько приёмов построения такого поля. Мы приведём построение Кантора.

Конструкция одного из изоморфных полей действительных чисел подсказывается теоремой 1. Если D — искомое поле, то каждый элемент поля D равен пределу фундаментальной последовательности рациональных чисел, и любая такая последовательность должна иметь предел в D в силу непрерывности поля.

За исходный элемент построения поля действительных чисел D мы принимаем фундаментальную последовательность рациональных чисел $a_1, a_2, a_3, \ldots = \{a_n\}$, т. е. последовательность, обладающую таким свойством: для любого рационального числа $\varepsilon > 0$ существует натуральное число n_0 такое, что $|a_p - a_q| < \varepsilon$ при любых p и q, бóльших n_0 (§ 24, определение 4). Пусть M — множество всех таких последовательностей. Определяем отношение эквивалентности, сложение и умножение последовательностей из M так, чтобы им соответствовали равенство, сложение и умножение элементов искомого поля D, равных пределам этих последовательностей [§ 24, теорема 2, а), б), в)], а именно,

$$\{a_n\} \sim \{b_n\} \tag{1}$$

тогда и только тогда, когда

$$\lim (a_n - b_n) = 0;$$

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}; \tag{2}$$

$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}. \tag{3}$$

Надо, конечно, доказать, что (2) и (3) действительно определяют операции во множестве M, т. е. что последовательности в правых частях этих равенств снова являются фундаментальными.

В случае сложения берём рациональное число $\varepsilon > 0$. Так как $\{a_n\}$ и $\{b_n\}$ фундаментальны, то существуют натуральные

числа n_1 и n_2 такие, что $|a_p - a_q| < \frac{\varepsilon}{2}$ при любых $p,\ q > n_1$ и $|b_p - b_q| < \frac{\varepsilon}{2}$ при любых $p,\ q > n_2$. Если n_0 — большее из чисел n_1, n_2, то

$$|(a_p + b_p) - (a_q + b_q)| \leqslant |a_p - a_q| + |b_p - b_q| < \varepsilon$$

при любых $p,\ q > n_0$, т. е. последовательность $\{a_n + b_n\}$ — фундаментальная.

В случае умножения сначала докажем, что любая фундаментальная последовательность $\{c_n\}$ ограничена (§ 24, определение 2). В самом деле существует n_0 такое, что $|c_p - c_q| < 1$ при любых $p,\ q > n_0$. Тогда

$$|c_n| = |(c_n - c_{n_0+1}) + c_{n_0+1}| \leqslant |c_n - c_{n_0+1}| + |c_{n_0+1}| < 1 + |c_{n_0+1}|$$

при любом $n > n_0$. Беря рациональное число c, большее всех чисел $|c_1|, |c_2|, \ldots, |c_{n_0}|, |c_{n_0+1}| + 1$ (например, сумму всех этих чисел плюс 1), получим $|c_n| < c$ при любом n.

Итак, существуют рациональные числа a и b такие, что $|a_n| < a$ и $|b_n| < b$ при любом n. Пусть дано рациональное число $\varepsilon > 0$. Существуют натуральные числа n_1 и n_2 такие, что $|a_p - a_q| < \frac{\varepsilon}{2b}$ при любых $p,\ q > n_1$ и $|b_p - b_q| < \frac{\varepsilon}{2a}$ при любых $p,\ q > n_2$. Если n_0 — большее из чисел n_1, n_2, то

$$|a_p b_p - a_q b_q| = |(a_p b_p - a_p b_q) + (a_p b_q - a_q b_q)| \leqslant$$
$$\leqslant |a_p| \cdot |b_p - b_q| + |b_q| \cdot |a_p - a_q| < a \cdot \frac{\varepsilon}{2a} + b \cdot \frac{\varepsilon}{2b} = \varepsilon$$

при любых $p,\ q > n_0$, т. е. последовательность $\{a_n b_n\}$ — фундаментальная.

Последовательность $\{a_n\}$ из M назовём положительной, если существуют рациональное число $\varepsilon > 0$ и натуральное число n_0 такие, что $a_n > \varepsilon$ при любом $n > n_0$.

Отношение эквивалентности последовательностей (1) обладает основными свойствами равенства (§ 19). Именно:

1) $\{a_n\} \sim \{a_n\}$, ибо $\lim (a_n - a_n) = 0$.

2) Если $\{a_n\} \sim \{b_n\}$, то $\{b_n\} \sim \{a_n\}$, ибо если $\lim (a_n - b_n) = 0$, то $\lim (b_n - a_n) = 0$ в силу $|a_n - b_n| = |b_n - a_n|$.

3) Если $\{a_n\} \sim \{b_n\}$ и $\{b_n\} \sim \{c_n\}$, то $\{a_n\} \sim \{c_n\}$, ибо если $\lim (a_n - b_n) = 0$ и $\lim (b_n - c_n) = 0$, то также

$$\lim (a_n - c_n) = \lim [(a_n - b_n) + (b_n - c_n)] =$$
$$= \lim (a_n - b_n) + \lim (b_n - c_n) = 0 + 0 = 0$$

[§ 24, теорема 2, б)].

По теореме из § 19 это отношение определяет разбиение множества M на классы эквивалентных последовательностей. Будем обозначать эти классы малыми греческими буквами α, β, γ, δ, ...

Определение 2. *Пусть D_0 есть множество всех классов, эквивалентных последовательностей множества M. Суммой (произведением) двух классов α и β назовём тот класс $\alpha+\beta$ (соответственно $\alpha\beta$), который содержит сумму (произведение) последовательности класса α и последовательности класса β. Класс α назовём положительным, если последовательность этого класса положительна.*

Покажем, что сумма, произведение и свойство класса быть положительным не зависят от выбора представителей данных классов. Пусть

$$\{a_n\}\sim\{b_n\} \quad \text{и} \quad \{c_n\}\sim\{d_n\}.$$

Тогда

$$\lim(a_n-b_n)=0 \quad \text{и} \quad \lim(c_n-d_n)=0,$$

откуда

$$\lim[(a_n+c_n)-(b_n+d_n)]=\lim(a_n-b_n)+\lim(c_n-d_n)=0,$$

т. е. $\{a_n+c_n\}\sim\{b_n+d_n\}$.

Так как последовательность $\{c_n\}$ — фундаментальная, то она ограничена. Поэтому существует рациональное число $c>0$ такое, что $|c_n|<c$ при любом n. Пусть теперь дано рациональное число $\varepsilon>0$. Существует n_0 такое, что $|a_n-b_n|<\frac{\varepsilon}{c}$ при любом $n>n_0$. Тогда

$$|a_nc_n-b_nc_n|=|a_n-b_n|\cdot|c_n|<\frac{\varepsilon}{c}\cdot c=\varepsilon$$

при любом $n>n_0$. Следовательно, $\lim(a_nc_n-b_nc_n)=0$, т. е.

$$\{a_nc_n\}\sim\{b_nc_n\}.$$

Применяя доказанное и очевидную коммутативность умножения последовательностей, находим:

$$\{a_nc_n\}\sim\{b_nc_n\}=\{c_nb_n\}\sim\{c_nd_n\}.$$

Наконец, если последовательность $\{a_n\}$ положительна и $\{a_n\}\sim\{b_n\}$, то существует рациональное $\varepsilon>0$ и натуральное n_1 такие, что $\{a_n\}>\varepsilon$ при любом $n>n_1$. Далее, для данного ε существует n_0 такое, что $|a_n-b_n|<\frac{\varepsilon}{2}$ при любом $n>n_2$. Если n_0 — большее из чисел n_1, n_2, то, применяя свойство абсолютных величин

$$|a-b|\geqslant||a|-|b||$$

[§ 10, (3)], находим

$$|b_n|=|a_n-(a_n-b_n)|\geqslant||a_n|-|a_n-b_n||=$$
$$=|a_n|-|a_n-b_n|>\varepsilon-\frac{\varepsilon}{2}=\frac{\varepsilon}{2}$$

при любом $n > n_0$, т. е. последовательность $\{b_n\}$ также положительна.

Итак, определение 2 действительно вводит во множество D_0 операцию сложения и умножения, и положительность класса из D_0 определяется любой из его последовательностей.

Теорема 4. *Множество D_0 при операциях сложения и умножения и определении положительности, указанных в определении 2, является непрерывным полем* (§ 24, определение 6).

Доказательство. Нужно проверить выполнение в D_0 всех свойств I—XII (см. § 7, определение 1, § 8, определение 1, § 10, определения 1 и 3, § 24, определение 5). Так как операции (2) и (3) над последовательностями определены через операции над их элементами, то из выполнения свойств кольца I—VI для рациональных чисел следует их выполнение для множества M, а потому и для множества D_0. Итак, M и D_0 — кольца.

Выясним, какой смысл имеют в кольце D_0 нуль и противоположный элемент. Очевидно, что нулём в D_0 будет класс, содержащий фундаментальную последовательность $\{0\} = 0, 0, 0, \ldots$ Мы его обозначим через (0). Этот класс состоит из всех последовательностей $\{a_n\}$, эквивалентных $\{0\}$, т. е. таких, для которых $\lim a_n = 0$. Мы будем называть их *нулевыми последовательностями.* Любая последовательность класса (0) эквивалентна $\{0\}$ и потому нулевая. Обратно, любая нулевая последовательность, как сходящаяся, фундаментальна и эквивалентна $\{0\}$, а потому принадлежит классу (0).

Класс $-\alpha$, противоположный классу α, содержащему последовательность $\{a_n\}$, содержит, очевидно, последовательность $\{-a_n\}$, противоположную $\{a_n\}$, и все последовательности, эквивалентные $\{-a_n\}$. Из $a_n - b_n = -[(-a_n) - (-b_n)]$ легко следует, что если $\{a_n\} \sim \{b_n\}$, то $\{-a_n\} \sim \{-b_n\}$, и обратно. Таким образом, класс $-\alpha$ состоит из всех последовательностей, противоположных последовательностям класса α.

Свойство VII поля уже не следует, как выше I—VI, прямо из аналогичного свойства чисел. В самом деле, если не все члены последовательности $\{a_n\}$ из M равны нулю, то $\{a_n\}$ отлична от последовательности $\{0\}$, являющейся нулём кольца M. Но если ещё $a_1 = 0$, то уравнение $\{a_n\} \cdot \{x_n\} = \{b_n\}$ при $b_1 \neq 0$ неразрешимо. Следовательно, кольцо M не является полем. Тем не менее D_0 будет полем. Пусть α и β — классы из D_0, причём $\alpha \neq (0)$. Берём $\{a_n\}$ из α и $\{b_n\}$ из β. Существуют рациональное число $a > 0$ и натуральное n_1 такие, что $|a_n| > a$ при любом $n > n_1$. Допуская противное, для любого $\varepsilon > 0$ найдём p такое, что $|a_n - a_q| < \frac{\varepsilon}{2}$ при любых $n, q > p$. Затем берём $q > p$ такое, что $|a_q| < \frac{\varepsilon}{2}$. Тогда получим

$$|a_n| = |(a_n - a_q) + a_q| \leqslant |a_n - a_q| + |a_q| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

при любом $n > p$. Это значит, что $\lim a_n = 0$. Но это невозможно, так как $\{a_n\}$ принадлежит классу $\alpha \neq (0)$.

Без ограничения общности можно считать $a_n \neq 0$ при любом n. В самом деле, в силу $|a_n| > a > 0$ при любом $n > n_1$, лишь конечное число членов a_n (при $n \leqslant n_1$) может равняться нулю. Заменяя их любыми рациональными числами, отличными от нуля, получим, очевидно, последовательность, эквивалентную $\{a_n\}$, т. е. принадлежащую классу α и не имеющую членов, равных нулю.

Покажем, что последовательность $\{c_n\} = \left\{\frac{b_n}{a_n}\right\}$ является фундаментальной. Последовательность $\{b_n\}$ как фундаментальная ограничена, т. е. существует рациональное число b такое, что $|b_n| < b$ при любом n. Пусть дано рациональное $\varepsilon > 0$. Так как $\{a_n\}$ и $\{b_n\}$ фундаментальны, то существуют натуральные n_2 и n_3 такие, что $|a_p - a_q| < \frac{a^2\varepsilon}{2b}$ при любых $p, q > n_2$ и $|b_p - b_q| < \frac{a\varepsilon}{2}$ при любых $p, q > n_3$. Пусть n_0 — наибольшее из чисел n_1, n_2 и n_3. Тогда

$$\left|\frac{b_p}{a_p} - \frac{b_q}{a_q}\right| = \left|\frac{b_p a_q - a_p b_q}{a_p a_q}\right| = \left|\frac{b_p a_q - a_p b_p}{a_p a_q} + \frac{a_p b_p - a_q b_q}{a_p a_q}\right| \leqslant$$

$$\leqslant \frac{|b_p| \cdot |a_q - a_p|}{|a_p| \cdot |a_q|} + \frac{|b_p - b_q|}{|a_q|} < \frac{b \cdot \frac{a^2\varepsilon}{2b}}{a^2} + \frac{\frac{a\varepsilon}{2}}{a} = \varepsilon$$

при любых $p, q > n_0$; таким образом, последовательность $\{c_n\} = \left\{\frac{b_n}{a_n}\right\}$ действительно фундаментальна.

Пусть γ — класс, содержащий $\{c_n\}$. Из $\{a_n\} \cdot \{c_n\} = \{b_n\}$ следует $\alpha\gamma = \beta$, чем свойство VII доказано.

Свойство VIII выполнено, ибо D_0 содержит, очевидно, более одного элемента.

Докажем выполнение в D_0 свойства IX. Надо показать, что для любого класса α имеет место один и только один из трёх случаев: α положителен, $-\alpha$ положителен, $\alpha = (0)$. Пусть ни α, ни $-\alpha$ не положительны. Берём последовательность $\{a_n\}$ класса α и рациональное число $\varepsilon > 0$. В силу фундаментальности $\{a_n\}$ существует n_0 такое, что $|a_p - a_q| < \frac{\varepsilon}{2}$ при любых $p, q > n_0$. Так как α не положителен, то существует $r > n_0$ такое, что $a_r \leqslant \frac{\varepsilon}{2}$. Так как $-\alpha$ не положителен и содержит последовательность $\{-a_n\}$, то существует $s > n_0$ такое, что $-a_s \leqslant \frac{\varepsilon}{2}$. Тогда при любом $n > n_0$ будет одновременно

$$a_n = a_r + (a_n - a_r) \leqslant a_r + |a_n - a_r| < \varepsilon$$

и

$$-a_n = (a_s - a_n) - a_s \leqslant |a_s - a_n| + (-a_s) < \varepsilon.$$

Поэтому $|a_n|<\varepsilon$ при любом $n>n_0$, т. е. $\lim a_n=0$, откуда $\alpha=(0)$.

Итак, один из трёх указанных выше случаев обязательно имеет место. Если класс α положителен, то существует рациональное $a>0$ и n_0 такие, что $a_n>a$, $-a_n<-a$ при любом $n>n_0$. Этим исключается как $\lim a_n=0$, т. е. $\alpha=(0)$, так и положительность класса $-\alpha$. Аналогично показывается, что положительность $-\alpha$ исключает два других случая. Этим уже доказано, что все три случая несовместимы, т. е. свойство IX выполнено.

Свойство X выполнено, так как сумма и произведение положительных последовательностей, очевидно, снова положительны.

Итак, доказано, что D_0 — расположенное поле. Считая $\alpha>\beta$, если $\alpha-\beta$ положительный класс, введём в D_0 порядок, при котором положительные элементы и только они будут больше нуля (§ 10, теорема 1).

Легко видеть, что единицей поля D_0 будет класс, содержащий последовательность $\{1\}=1, 1, 1, \ldots$ и все последовательности $\{a_n\}$, ей эквивалентные, т. е. такие, для которых $\lim a_n=1$. Будем обозначать этот класс через (1).

Покажем, что в D_0 выполнена аксиома Архимеда XI. Пусть класс α содержит последовательность $\{a_n\}$. Выше мы показали, что фундаментальная последовательность ограничена. Поэтому существует рациональное число a такое, что $|a_n|<a$ и потому $a-a_n>0$ при любом n. Так как в поле рациональных чисел аксиома Архимеда выполнена (§ 23, теорема 3), то существует натуральное число $k>a+1$. Тогда $k-a_n>1$ при любом n и, следовательно, класс $k\cdot(1)-\alpha$ положителен, т. е. $k\cdot(1)>\alpha$. Отсюда для поля D_0 вытекает XI.

Наконец, покажем, что в D_0 выполнена аксиома полноты XII (§ 24, определение 5). Заметим сначала, что если класс α содержит последовательность $\{a_n\}$, где $a_n\geqslant 0$ при любом n, большем некоторого натурального числа n_0, то $\alpha\geqslant(0)$, так как, очевидно, неравенство $\alpha<(0)$ невозможно. Поэтому, если α содержит $\{a_n\}$ и β содержит $\{b_n\}$, то из $a_n\geqslant b_n$ при любом $n>n_0$ следует $\alpha\geqslant\beta$. Аналогично тому, как классы, содержащие последовательности $\{0\}$ и $\{1\}$, мы обозначили через (0) и (1), мы теперь для любого рационального числа a обозначим через (a) класс, содержащий последовательность $\{a\}=a, a, a, \ldots$. Такие последовательности, все члены которых равны, мы будем называть *стационарными*. Очевидно, что соответствие $a\longleftrightarrow(a)$ является изоморфным отображением поля Γ рациональных чисел на множество Γ' всех классов, содержащих стационарные последовательности. Следовательно, Γ' также является полем (§ 9, теорема 1).

В поле D_0, как в любом архимедовски расположенном поле, определены понятия предела и фундаментальной последовательности,

не меняющие смысла при переходе к подполю (§ 24, определения 3 и 4, замечание и теорема 5).

Покажем, что если класс α содержит последовательность $\{a_n\}$, то $\lim(a_n)=\alpha$. Пусть $\varepsilon>(0)$ — элемент поля D_0, содержащий последовательность $\{e_n\}$. Тогда существует рациональное число $e>0$ и натуральное m такие, что $e_n>e$ при любом $n>m$, т. е. $\varepsilon\geqslant(e)$. Берём рациональное число ε' такое, что $e>\varepsilon'>0$ (например, $\varepsilon'=\frac{e}{2}$). Тогда $(\varepsilon')<(e)\leqslant\varepsilon$. Так как последовательность $\{a_n\}$ фундаментальна, то существует натуральное n_0 такое, что $|a_p-a_q|<\varepsilon'$ при любых $p,\ q>n_0$. Поэтому для данного $n>n_0$ будем иметь: $a_p-a_n<\varepsilon'$ и $a_n-a_q<\varepsilon'$ при любых $p,\ q>n_0$. Переходя при данном n от последовательностей к содержащим их классам, по доказанному выше получим:

$$\alpha-(a_n)<(\varepsilon') \quad \text{и} \quad (a_n)-\alpha<(\varepsilon'),$$

откуда $|(a_n)-\alpha|<(\varepsilon')<\varepsilon$ при любом $n>n_0$; это и означает, что $\lim(a_n)=\alpha$.

Мы доказали, что любая фундаментальная последовательность элементов (a_n) подполя Γ' имеет предел в D_0. Отсюда уже нетрудно вывести полноту поля D_0. Пусть $\{a_n\}$ — любая фундаментальная последовательность элементов поля D_0. Так как по доказанному каждый класс α_n равен пределу классов из подполя Γ', то для данного n [ввиду $\left(\frac{1}{n}\right)>(0)$] существует элемент (a_n) из Γ' такой, что $|\alpha_n-(a_n)|<\left(\frac{1}{n}\right)$. Покажем, что последовательность $\{(a_n)\}$ фундаментальна. Пусть $\varepsilon>(0)$ — любой элемент D_0. Как было показано выше, из аксиомы Архимеда вытекает, что существует рациональное число $e>0$ такое, что $(e)<\varepsilon$. Существует натуральное $n_1>\frac{3}{e}$ или $\frac{1}{n_1}<\frac{e}{3}$. Далее, в силу фундаментальности $\{a_n\}$ существует натуральное n_2 такое, что $|a_p-a_q|<\left(\frac{e}{3}\right)$ при любых $p,q>n_2$. Если n_0 — большее из чисел n_1 и n_2, то

$$|(a_p)-(a_q)|\leqslant|(a_p)-a_p|+|a_p-a_q|+|a_q-(a_q)|<$$
$$<\left(\frac{1}{p}\right)+\left(\frac{e}{3}\right)+\left(\frac{1}{q}\right)<\left(\frac{e}{3}\right)+\left(\frac{e}{3}\right)+\left(\frac{e}{3}\right)=(e)<\varepsilon$$

при любых $p,\ q>n_0$.

Из изоморфизма полей Γ и Γ' (сохраняющего, очевидно, отношения порядка) вытекает, что последовательность $\{a_n\}$ рациональных чисел сама фундаментальна. Пусть α — класс из D_0, содержащий $\{a_n\}$. Выше было доказано, что $\lim(a_n)=\alpha$. Но $\lim[(a_n)-a_n]=0$.

В самом деле, для любого $\varepsilon > 0$ из D_0 берём рациональное $e > 0$ такое, что $(e) < \varepsilon$, и натуральное n_0 такое, что $\frac{1}{n_0} < e$. Тогда $|(a_n) - \alpha_n| < \left(\frac{1}{n}\right) < (e) < \varepsilon$ при любом $n > n_0$. Таким образом, последовательность $\{\alpha_n\}$ также сходится и притом

$$\lim \alpha_n = \lim (a_n) = \alpha.$$

Этим доказано свойство XII, а значит, и теорема 4.

Поле D_0 с точностью до изоморфизма и является полем действительных чисел. Однако оно не содержит поля рациональных чисел Г, от которого мы отправлялись при его построении. Элементами поля D являются классы эквивалентных фундаментальных последовательностей рациональных чисел, но не сами рациональные числа.

Но выше мы видели, что D_0 содержит подполе Г′ классов, содержащих стационарные последовательности, изоморфное Г. Поэтому существует поле D, содержащее поле Г в качестве подполя и изоморфное (относительно сложения и умножения) полю D (§ 9, теорема 2). Перенесём отношения порядка с D_0 на D при помощи данного изоморфного отображения f поля D на D_0. Именно, элемент d поля D будем считать положительным, если соответствующий ему элемент $f(d) = d_0$ поля D_0 положителен. Тогда поле D будет расположено, и данный изоморфизм f сохраняет отношения порядка. Порядок D порождает порядок его подполя Г, совпадающий с определённым прежде для рациональных чисел, ибо поле Г вообще допускает единственное расположение (§ 23, теорема 1). При изоморфизме D и D_0 поле Г изоморфно отображается на некотором подполе Г″ из D_0. Но так как Г изоморфно Г′ и Г допускает единственное изоморфное отображение в D_0 (§ 23, теорема 2), то Г″ = Г′, и при изоморфизме D и D_0 рациональному числу a из Г соответствует класс (a) из Г′.

Из сохранения отношений порядка при изоморфизме D и D_0 следуют для поля D: сохранение всех свойств расположения, в частности выполнение аксиомы Архимеда, совпадение фундаментальности и сходимости последовательностей и полнота. Стало быть, из непрерывности поля D_0 следует непрерывность поля D.

Итак, поле действительных чисел D построено. Его элементами, т. е. действительными числами, являются, во-первых, все рациональные числа и, во-вторых, классы эквивалентных и не имеющих рационального предела фундаментальных последовательностей рациональных чисел.

Из свойств поля D_0 вытекает, что любая фундаментальная последовательность $\{a_n\}$ рациональных чисел имеет своим пределом в D либо рациональное число, либо тот класс, которому принадлежит данная последовательность $\{a_n\}$.

§ 26. Свойства действительных чисел

Поле действительных чисел D обладает всеми свойствами расположенных полей, доказанными в главе II. Так, в этом поле отсутствуют делители нуля (§ 7, определение 2 и теорема 2, § 8, теорема 1). Имеют смысл понятия положительного и отрицательного чисел (§ 10, определение 1) и вводится порядок, при котором нуль меньше всех положительных и больше всех отрицательных чисел (§ 10, теорема 1). Справедливы закон монотонности и обычные правила оперирования с неравенствами (§ 10, теоремы 2—4). Квадрат любого числа, кроме нуля, положителен (§ 10, теорема 7). Имеет смысл понятие абсолютной величины (§ 10, определение 2), причём абсолютная величина обладает обычными свойствами и верны обычные правила сравнения и оперирования над членами через сравнение и оперирование над их абсолютными величинами (§ 10, теорема 8 и следующие за ней замечания).

Действительные числа, не являющиеся рациональными, называются *иррациональными.*

Переходим к задаче об извлечении корня из любого действительного числа. Решение этой задачи мы получим, рассмотрев гораздо более общую задачу о нахождении значения аргумента, при котором непрерывная функция принимает данное значение. Понятие о непрерывной функции, связанное с понятием предела последовательности, играет основную роль во всём математическом анализе.

Общее понятие функции нам уже известно (§ 3, определение 1). Здесь мы будем рассматривать лишь функции, связанные с полем действительных чисел.

Определение 1. *Действительной функцией* (или *функцией действительного переменного*) $y=f(x)$ (или короче f), *заданной на множестве* X *действительных чисел, называется соответствие, сопоставляющее с каждым числом* x *множества* X *одно определённое действительное число* $y=f(x)$. *Число* x *называется значением аргумента, а* y *— значением функции при данном значении аргумента* x (или *в точке* x).

Всюду в этом параграфе под функциями мы, не оговаривая этого, будем понимать действительные функции.

Определение 2. *Функция* $y=f(x)$, *заданная на множестве* X *действительных чисел, называется непрерывной в точке* x_0 *множества* X, *если для любого действительного числа* $\varepsilon>0$ *существует действительное число* $\delta>0$ *такое, что из* $|x-x_0|<\delta$ *следует* $|f(x)-f(x_0)|<\varepsilon$ *для любого числа* x *множества* X. *Функция* $y=f(x)$ *называется непрерывной на множестве, если она непрерывна в каждой его точке* (т. е. для любого числа x_0 из X).

Связь понятия непрерывности функции с понятием предела определяется теоремой:

Теорема 1. *Функция f, заданная на множестве X, тогда и только тогда непрерывна в точке x_0 из X, когда из $\lim\limits_{n\to\infty} x_n = x_0$ следует $\lim\limits_{n\to\infty} f(x_n) = f(x_0)$ для любой последовательности $\{x_n\}$ множества X. Функция $f(x)$ тогда и только тогда непрерывна на множестве X, если из $\lim\limits_{n\to\infty} x_n = x_0$ следует $\lim\limits_{n\to\infty} f(x_n) = f(x_0)$ для любого числа x_0 из X и любой последовательности $\{x_n\}$ чисел множества X.*

Доказательство. Достаточно, очевидно, доказать часть теоремы, относящуюся к непрерывности в точке.

а) Пусть $f(x)$ непрерывна в точке x_0 и $\lim x_n = x_0$. Берём любое число $\varepsilon > 0$. По определению непрерывности существует число $\delta > 0$ такое, что из $|x - x_0| < \delta$ следует $|f(x) - f(x_0)| < \varepsilon$ для любого x из X. По определению предела (§ 24, определение 3) для этого числа δ существует натуральное число n_0 такое, что $|x_n - x_0| < \delta$ при любом $n > n_0$. По выбору числа δ отсюда следует, что $|f(x_n) - f(x_0)| < \varepsilon$ при любом $n > n_0$. По определению предела это значит, что

$$\lim_{n\to\infty} f(x_n) = f(x_0).$$

б) Пусть $\lim\limits_{n\to\infty} f(x_n) = f(x_0)$ для любой последовательности $\{x_n\}$ из X. Если функция $f(x)$ не является непрерывной в точке x_0, то существует число $\varepsilon > 0$, для которого нельзя найти числа δ с требуемым в определении 2 свойством. Иными словами, при выбранном таким образом ε для любого числа $\delta > 0$ существует число x множества X такое, что $|x - x_0| < \delta$, но $|f(x) - f(x_0)| \geqslant \varepsilon$. Поэтому для любого натурального числа n существует число x_n из X такое, что

$$|x_n - x_0| < \frac{1}{n}, \tag{1}$$

$$|f(x_n) - f(x_0)| \geqslant \varepsilon \tag{2}$$

при любом n.

Так как поле действительных чисел по определению архимедовски расположено (§ 25, определение 1), то для любого действительного числа $\varepsilon_0 > 0$ существует натуральное $n_0 > \frac{1}{\varepsilon_0}$. Тогда из (1) находим $|x_n - x_0| < \frac{1}{n} < \frac{1}{n_0} < \varepsilon_0$ при любом $n > n_0$, т. е. $\lim x_n = x_0$. По условию тогда также $\lim f(x_n) = f(x_0)$, что, очевидно, противоречит (2). Таким образом, $f(x)$ непрерывна в точке x_0.

Определим сумму, разность, произведение и частное двух функций $f_1(x)$ и $f_2(x)$, заданных на множестве X, как функцию, сопоставляющую с каждым числом x из X соответственно сумму, разность, произведение и частное значений данных функций в точке x, т. е.

$f(x)$ равна соответственно

$$f_1(x)+f_2(x),\quad f_1(x)-f_2(x),\quad f_1(x)\cdot f_2(x),\quad \frac{f_1(x)}{f_2(x)}$$

для любого числа x из X (в случае частного предполагается, что $f_2(x)\neq 0$ для любого x из X).

Из теоремы 1 и свойств предела [§ 24, теорема 2, б), в), г)] непосредственно следует

Теорема 2. *Сумма, разность и произведение двух функций f_1 и f_2, непрерывных на множестве X, также непрерывны на множестве X. Частное функций f_1 и f_2, непрерывных на множестве X, есть функция, непрерывная на множестве X' тех чисел x из X, для которых $f_2(x)\neq 0$.*

Рассмотрим примеры непрерывных функций.

Пример 1. Функция $f(x)=x^k$ для любого целого числа $k\geqq 0$ определена и непрерывна на множестве всех действительных чисел. В самом деле, при $k=0$ функция $f(x)=1$ при любом x и непрерывна как любая константа, ибо $|f(x)-f(x_0)|=0$; очевидно, непрерывна и функция $f(x)=x$. Применяя теорему 2, легко доказать непрерывность функции x^k индукцией по k.

Пример 2. Из примера 1 и теоремы 3 индукцией по числу членов получаем непрерывность на множестве всех действительных чисел функции, заданной многочленом $f(x)=a_0+a_1x+\ldots+a_nx^n$ с действительными коэффициентами $a_0, a_1, \ldots, a_n$. Отсюда опять по теореме 2 получается непрерывность функции, заданной на множестве X всех чисел x, для которых $g(x)\neq 0$, дробью $\frac{f(x)}{g(x)}$, где $f(x)$ и $g(x)$ — многочлены с действительными коэффициентами. Сами эти функции называются многочленами или целыми рациональными функциями и, соответственно, дробными рациональными функциями.

Пример 3. Функции $\sin x$ и $\cos x$ непрерывны на множестве всех действительных чисел. Функция $\operatorname{tg} x$ непрерывна во всех точках, где она определена, т. е. где $\cos x\neq 0$. Функция $\operatorname{ctg} x$ непрерывна во всех точках, где $\sin x\neq 0$. Чтобы доказать это, надо дать точное определение указанных функций. Любой угол α как геометрическая фигура определяет дугу круга радиуса 1. Так как поле действительных чисел непрерывно, то в нём существует число x, равное длине данной дуги. Это число x называется *радианной мерой угла* α. Обратно, для данного числа x можно построить дугу длины x, а для неё — центральный угол α. Тогда угол α будет иметь радианную меру x. Если ввести углы, бóльшие 360°, и отрицательные углы, как это обычно делается, то можно установить взаимно однозначное соответствие между всеми действительными числами и всеми углами, при котором числу x соответствует угол α с радианной мерой x. Поэтому обычно под углом и понимают не геометрическую фигуру, а число, равное радианной мере угла. Тогда $\sin x$ определяется как функция, сопоставляющая с любым действи-

тельным числом x действительное число, равное отношению линии синусов к радиусу круга при известном из тригонометрии соглашении о знаках. Также определяются другие тригонометрические функции. Подчёркиваем ещё раз, что трудность принципиального характера при таком определении тригонометрических функций лежит в задаче об измерении дуг окружности, которая разрешима в поле действительных чисел благодаря непрерывности поля [1]).

Отметим, что соответствие между углами и их радианными мерами таково, что сумме углов $\alpha+\beta$ соответствует сумма $x+y$ их радианных мер и произведению $a\alpha$ угла α на число a соответствует произведение ax радианной меры x угла на то же число a. Отсюда можно вывести, что все тригонометрические формулы, доказанные для функций углов, остаются верными для функций от радианных мер этих углов.

Для доказательства непрерывности $\sin x$ убедимся, что $|\sin x| \leqslant |x|$ при любом действительном x. Так как $\sin(-x) = -\sin x$, то достаточно рассмотреть числа $x \geqslant 0$, а так как $|\sin x| \leqslant 1$, то достаточно рассмотреть числа x, для которых $0 \leqslant x \leqslant \frac{\pi}{2}$. Эти углы лежат в первой четверти. Очевидно, линия синусов MP равна половине хорды MN, стягивающей дугу $MAN = 2x$ (рис. 1). Но все ломаные, вписанные в дугу MAN, длиннее хорды MN. А потому длина $2x$ дуги MAN как предел последовательности длин вписанных хорд не меньше длины хорды MN.

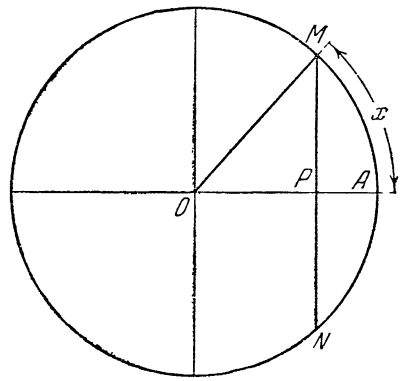


Рис. 1.

Итак, $MN \leqslant 2x$, $\frac{MN}{2} \leqslant x$, т. е. $\sin x \leqslant x$. Но $x \geqslant 0$ и $\sin x \geqslant 0$. Поэтому $|\sin x| \leqslant |x|$.

Пусть дано действительное число $\varepsilon > 0$. Положим: $\delta = \frac{\varepsilon}{2}$. Тогда, применяя формулу

$$\sin\alpha - \sin\beta = 2\cos\frac{\alpha+\beta}{2} \cdot \sin\frac{\alpha-\beta}{2}$$

и неравенство $|\cos\alpha| \leqslant 1$, находим, что из $|x - x_0| < \delta$ следует:

$$|\sin x - \sin x_0| = \left|2\cos\frac{x+x_0}{2} \cdot \sin\frac{x-x_0}{2}\right| \leqslant 2|x - x_0| < 2\delta = \varepsilon,$$

что и доказывает непрерывность $\sin x$.

[1]) В курсах математического анализа даётся другое определение этих функций (с помощью бесконечных рядов), не опирающееся на измерение дуг и на геометрию вообще.

Непрерывность $\cos x$ доказывается аналогично или проще выводится из соотношения $\cos x = \sin\left(\frac{\pi}{2} - x\right)$. Из непрерывности синуса и косинуса по теореме 2 следует непрерывность тангенса и котангенса во всех точках x, где они определены.

Из этих примеров видно, насколько широким является класс непрерывных функций. Для всех таких функций мы докажем следующее предложение.

Теорема 3. (Теорема о промежуточном значении.) *Пусть $f(x)$ — функция, заданная и непрерывная на отрезке* $[a, b]$ (т. е. на множестве действительных чисел x, для которых $a \leqslant x \leqslant b$, см. конец § 1). *Пусть, далее, $f(a) = \alpha$ и $f(b) = \beta$. Тогда для любого числа γ, принадлежащего отрезку* $[\alpha, \beta]$ (при $\alpha \leqslant \beta$) или отрезку $[\beta, \alpha]$ (при $\beta \leqslant \alpha$), *существует число c отрезка* $[a, b]$ *такое, что $f(c) = \gamma$.* Иными словами, *функция, заданная и непрерывная на некотором отрезке, принимает на этом отрезке все значения, промежуточные по отношению к её значениям в концах отрезка.*

Доказательство. Если $\alpha = \beta$, то $\alpha = \gamma = \beta$, и можно положить: $c = a$ или $c = b$. Пусть $\alpha < \beta$ (в случае $\beta < \alpha$ доказательство аналогично). Если $\gamma = \beta$, то можно положить: $c = b$. Итак, пусть $\alpha \leqslant \gamma < \beta$. Применим весьма распространённый метод деления отрезка пополам. Строим две последовательности действительных чисел $\{a_n\}$ и $\{b_n\}$, принадлежащие отрезку $[a, b]$ и обладающие свойствами

$$f(a_n) \leqslant \gamma < f(b_n), \tag{3}$$

$$a_n \leqslant a_{n+1}, \quad b_n \geqslant b_{n+1}, \tag{4}$$

$$b_n - a_n = \frac{b-a}{2^n} \tag{5}$$

для любого натурального числа n.

Положим: $a_1 = a$, $b_1 = b$. Если уже определены числа a_n и b_n отрезка $[a, b]$, то число $\frac{a_n + b_n}{2}$ также принадлежит отрезку $[a, b]$, и значит, для этого числа функция f определена. Если

$$f\left(\frac{a_n + b_n}{2}\right) \leqslant \gamma,$$

то положим: $a_{n+1} = \frac{a_n + b_n}{2}$ и $b_{n+1} = b$. Если же

$$f\left(\frac{a_n + b_n}{2}\right) > \gamma,$$

то положим:

$$a_{n+1} = a_n \quad \text{и} \quad b_{n+1} = \frac{a_n + b_n}{2}.$$

Этими свойствами последовательности $\{a_n\}$ и $\{b_n\}$ однозначно опре-

делены (§ 15, теорема 1). Покажем, что выполнены свойства (3), (4), (5). Выполнение свойства (4) непосредственно следует из определения чисел a_{n+1} и b_{n+1}. Выполнение свойств (3) и (5) докажем индукцией по n. Так как $\alpha \leqslant \gamma < \beta$, то эти свойства выполнены при $n=1$. Пусть они выполнены для числа n, т. е. $f(a_n) \leqslant \gamma < f(b_n)$ и $b_n - a_n = \frac{b-a}{2^n}$. Тогда по определению a_{n+1} и b_{n+1}, очевидно,

$$f(a_{n+1}) \leqslant \gamma < f(b_{n+1}),\quad b_{n+1} - a_{n+1} = \frac{b_n - a_n}{2} = \frac{b-a}{2^{n+1}}.$$

Из (4) вытекает, что если $p < q$, то $a_p \leqslant a_q$. Покажем, что $\{a_n\}$ есть фундаментальная последовательность. Так как поле действительных чисел архимедовски расположено, то для любого числа $\varepsilon > 0$ существует натуральное число n_0 такое, что $\frac{1}{2^{n_0}} < \frac{\varepsilon}{b-a}$ (§ 23, теорема 5) и $\frac{b-a}{2^{n_0}} < \varepsilon$ (из $\alpha \neq \beta$ следует $a \neq b$, т. е. $b - a > 0$). Тогда, если $p \leqslant q$, то

$$|a_p - a_q| = a_q - a_p < b_p - a_p = \frac{b-a}{2^p} < \varepsilon$$

при любых p, $q > n_0$.

В силу полноты поля действительных чисел последовательность $\{a_n\}$ имеет предел c. Из (5) (снова применяя теорему 5 из § 23) легко находим, что $\lim(a_n - b_n) = 0$, а потому последовательность $\{b_n\}$ также сходится, причём $\lim a_n = \lim b_n = c$ [§ 24, теорема 2, а)].

Так как функция $f(x)$ непрерывна на отрезке $[a, b]$, то по теореме 1 находим: $\lim f(a_n) = \lim f(b_n) = f(c)$. Но из (3) получаем: $\lim f(a_n) \leqslant \gamma \leqslant \lim f(b_n)$ [§ 24, теорема 2, д)], или $f(c) \leqslant \gamma \leqslant f(c)$, $f(c) = \gamma$, что и требовалось доказать.

Из многочисленных приложений этой теоремы укажем лишь на извлечение корня и определение угла по значению синуса, что будет использовано в следующей главе.

Теорема 4. *Для любого действительного числа $a > 0$ и любого натурального числа n существует одно и только одно действительное число $b > 0$ такое, что $b^n = a$. Иными словами, $\sqrt[n]{a}$ имеет одно и только одно положительное значение b. Если n чётно, то этот корень имеет ещё одно и только одно отрицательное значение $-b$ с той же абсолютной величиной. Если $a = 0$, то единственное значение корня будет $\sqrt[n]{a} = 0$. Если $a < 0$, то при нечётном n существует одно и только одно действительное значение корня и притом отрицательное, а при чётном n в поле действительных чисел $\sqrt[n]{a}$ значений не имеет.*

Доказательство. Функция $f(x) = x^n$ задана и непрерывна на множестве всех действительных чисел, а следовательно, на любом отрезке. Пусть $a > 0$. Берём число $c = a + 1$. Из $c > 1 > 0$ следует

$c^{n-1} \geqslant 1$ (знак $=$ получим лишь при $n=1$) и $c^n \geqslant c > a$. Применим теорему о промежуточном значении функции x^n на отрезке $[0, c]$. Так как $0^n < a < c^n$, то существует число b отрезка $[0, c]$, для которого $b^n = a$, $\sqrt[n]{a} = b$. Очевидно, $b > 0$. Если также $b' > 0$ и $b' \neq b$, то при $b' < b$ будет $b'^n < b^n$, а при $b' > b$ будет $b'^n > b^n$ (§ 10, теорема 4), т. е. $b'^n \neq a$, чем доказана единственность положительного значения $\sqrt[n]{a}$. При чётном n также

$$(-b)^n = [(-b)^2]^{\frac{n}{2}} = (b^2)^{\frac{n}{2}} = b^n = a,$$

т. е. $-b$ есть другое значение корня. Если $b' < 0$ и $b' \neq -b$, то при $b' < -b$ будет: $b'^2 > b^2 > 0$, откуда

$$b'^n = (b'^2)^{\frac{n}{2}} > (b^2)^{\frac{n}{2}} = b^n = a.$$

Аналогично при $-b < b' < 0$ будет: $b'^n < a$. Этим доказана единственность отрицательного значения $-b = \sqrt[n]{a}$.

Если n нечётно, то $\sqrt[n]{a}$ отрицательных значений не имеет, ибо из $b' < 0$ следует: $b'^n < 0 < a$.

Если $a = 0$, то $0^n = 0 = a$. Других значений $\sqrt[n]{0}$ не имеет, ибо из $b^n = 0$ следует $b = 0$, так как поле не имеет делителей нуля.

Если $a < 0$ и n нечётно, то по доказанному выше существует одно и только одно число b и притом положительное, для которого $b^n = -a$. Тогда

$$(-b)^n = (-1)^n b^n = a.$$

Если $b' \neq -b$, то, как и выше, убедимся, что $b'^n \neq (-b)^n = a$.

Итак, $\sqrt[n]{a}$ имеет единственное значение $-b$.

Наконец, если $a < 0$ и n чётно, то $\sqrt[n]{a}$ не имеет значений в поле действительных чисел. В самом деле, так как поле действительных чисел является расположенным полем (§ 10, определение 1), то для любого числа b должно быть $b^2 \geqslant 0$ (§ 10, теорема 7). Поэтому $b^n = (b^2)^{\frac{n}{2}} \geqslant 0$, т. е. $b^n \neq a$.

Остановимся на разыскании угла по значению его синуса.

Теорема 5. *Для любого числа a отрезка* $[0, 1]$ *существует одно и только одно число b отрезка* $\left[0, \frac{\pi}{2}\right]$ *такое, что* $a = \sin b$.

Доказательство. Функция $f(x) = \sin x$ задана и непрерывна на множестве всех действительных чисел, а следовательно, на отрезке $\left[0, \frac{\pi}{2}\right]$. Так как $\sin 0 \leqslant a \leqslant \sin \frac{\pi}{2}$, то по теореме о промежуточном значении существует число b отрезка $\left[0, \frac{\pi}{2}\right]$, для кото-

рого $\sin b = a$. Для доказательства единственности числа b воспользуемся свойством функции $\sin x$ возрастать с ростом угла от нуля до $\frac{\pi}{2}$. Это известно из тригонометрии и доказывается так: если $0 \leqslant x_1 < x_2 \leqslant \frac{\pi}{2}$, то большему углу соответствует и бóльшая дуга, но $0 < 2x_1 < 2x_2 \leqslant \pi$, и для таких дуг бóльшая дуга стягивается большей хордой. Половина хорды, стягивающей дугу длины $2x$, является линией синусов угла x. Отсюда ясно, что $\sin x_1 < \sin x_2$. Если теперь $b' \neq b$ — другое число отрезка $\left[0, \frac{\pi}{2}\right]$, то при $b < b'$ будет: $\sin b < \sin b'$, а при $b' < b$ будет: $-\sin b' < \sin b$. Следовательно, $\sin b' \neq a$.

Рассмотрим в заключение этого параграфа некоторые свойства поля действительных чисел как непрерывно расположенного поля.

Теорема 6. *Поле действительных чисел D может быть расположено лишь одним способом* (при сохранении операций сложения и умножения) *и допускает лишь одно изоморфное* (относительно сложения и умножения) *отображение в себя, а именно, тождественное отображение на самого себя.*

Доказательство. Пусть D — поле действительных чисел, расположенное обычным образом (§ 25, определение 2 и ниже), и D' — поле, совпадающее с D по составу элементов и по операциям сложения и умножения, но расположенное произвольным образом. Из совпадения сложения следует, что нуль поля D будет нулём и в D'. Далее, если $a > 0$ в D, то по теореме 4 существует число b такое, что $a = b^2$ в D, а по совпадению умножения — и в D'. Так как D' — расположенное поле, то его элемент a как квадрат элемента b положителен (§ 10, теорема 7), ибо $a \neq 0$, т. е. $a > 0$ в D'. Если $a < 0$ в D, то $-a > 0$ в D, а поэтому и в D', т. е. $a < 0$ также в D'. Отсюда следует, что если $a > 0$ в D', то $a > 0$ в D, ибо исключено, что $a \leqslant 0$ в D. Таким образом, a тогда и только тогда положительно в D', когда оно положительно в D, т. е. расположенное поле D' совпадает с D; поле D допускает лишь одно расположение.

Пусть $x' = f(x)$ — любое изоморфное (относительно сложения и умножения) отображение поля действительных чисел D на некоторое его подполе P. Если число $a > 0$, то $a = b^2$, где $b \neq 0$. В силу свойств изоморфизма тогда

$$a' = f(a) = f(b^2) = [f(b)]^2 > 0,$$

т. е. при изоморфизме f положительное число переходит в положительное.

Между двумя различными действительными числами a и b всегда лежит рациональное число c.

В самом деле, пусть $a<b$, $b-a>0$. По аксиоме Архимеда существует натуральное число $n>\frac{1}{b-a}$; тогда $\frac{1}{n}<b-a$. Далее, существуют натуральные числа m_1 и m_2, для которых

$$m_1\cdot\frac{1}{n}>a \quad \text{и} \quad m_2\cdot\frac{1}{n}>-a,$$

т. е. $(-m_2)\frac{1}{n}<a$. Поэтому множество A тех целых чисел k, для которых $k\cdot\frac{1}{n}>a$, непусто (ибо содержит m_1) и ограничено снизу числом $-m_2$. Следовательно, оно содержит наименьшее число m (§ 21, теорема 5). Тогда $\frac{m-1}{n}\leqslant a<\frac{m}{n}$, откуда

$$a<\frac{m}{n}=\frac{m-1}{n}+\frac{1}{n}<a+(b-a)=b,$$

т. е. рациональное число $\frac{m}{n}$ лежит между a и b.

При изоморфном отображении f поля D в себя поле рациональных чисел тождественно отображается на себя (§ 23, теорема 2). Если бы отображение f не было тождественным отображением поля D на себя, то существовало бы действительное число a такое, что $f(a)=b\neq a$. Пусть, например, $a<b$. По доказанному существует рациональное число c такое, что $a<c<b$, откуда

$$a-c<0<b-c \quad \text{и} \quad c-a>0>c-b.$$

Но

$$f(c-a)=f(c)-f(a)=c-b,$$

т. е. число $c-a>0$ перешло в число $c-b<0$, что невозможно.

Оперировать с действительными числами как классами фундаментальных последовательностей рациональных чисел практически неудобно ввиду громоздкости такого изображения. На практике при вычислениях с действительными числами применяется их запись десятичными дробями [1]).

§ 27. Аксиоматическое определение действительных чисел

Совокупность натуральных чисел мы определили при помощи основного отношения «следует», подчинённого системе аксиом Пеано (§ 11, определение 1). Такое построение математической теории является аксиоматическим. Далее, с помощью натуральных чисел мы последовательно определили целые, рациональные и действительные числа. Во всех этих трёх случаях новая числовая об-

[1]) См. статью А. Я. Хинчина «Элементы теории чисел», гл. IV.

ласть определялась через старую при помощи наложения дополнительных требований, обеспечивающих однозначное до изоморфизма определение новой области. Каждый раз мы строили интерпретацию (конкретный пример) определяемой области. Ввиду изоморфизма всех множеств, удовлетворяющих данному определению, мы могли бы в каждом случае саму интерпретацию принять за определение данной области. Такое определение числовых областей называется *конструктивным*. Возникает вопрос, можно ли определить каждую из упомянутых областей аксиоматически?

Расширяя числовую область, мы каждый раз налагали новые требования (возможность вычитания, деления и, наконец, непрерывность) при условии минимальности расширения. В отношении действительных чисел требование минимальности оказалось уже излишним. Это означает, что совокупность свойств, предъявленных ко множеству действительных чисел, характеризует это множество однозначно до изоморфизма. Тем самым эта совокупность свойств даёт аксиоматическое определение действительных чисел. Таким образом, определение действительных чисел как непрерывного расположенного поля является их аксиоматическим определением. Собирая вместе все свойства, включённые в это понятие, приходим к такому определению.

Определение. *Полем действительных чисел называется непустое множество D, в котором двум любым элементам a и b соответствуют элемент $a+b$, называемый их суммой, и элемент ab, называемый их произведением, и определено свойство элемента быть положительным, причём выполнены условия*:

I. (Коммутативность сложения.) $a+b=b+a$.

II. (Ассоциативность сложения.) $a+(b+c)=(a+b)+c$.

III. (Обратимость сложения.) *Для любых элементов a и b множества D существует элемент c из D такой, что* $a+c=b$.

IV. (Коммутативность умножения.) $ab=ba$.

V. (Ассоциативность умножения.) $a(bc)=(ab)c$.

VI. (Дистрибутивность умножения относительно сложения.) $(a+b)c=ab+bc$.

Эти свойства означают, что D есть кольцо. Стало быть, определено умножение элементов D на натуральные числа; существует единственный элемент 0 такой, что $a+0=0+a=a$ для любого a из D; для данного a существует единственный противоположный элемент $-a$ такой, что $a+(-a)=(-a)+a=0$; для данных a и b существует единственный элемент $b-a$, называемый их *разностью*, такой, что $a+(b-a)=(b-a)+a=b$.

Далее:

VII. (Обратимость умножения.) *Для любых элементов a и b множества D, где $a\neq 0$, существует элемент q из D такой, что* $aq=b$.

VIII. (Аксиома мощности.) *Множество D содержит по крайней мере два различных элемента.*

Условия I — VIII означают, что D — поле (§ 8, определение 1). Стало быть, определено понятие подполя поля D (§ 8, определение 3). Далее:

IX. *Для любого элемента a множества D имеет место один и только один из трёх случаев: a положителен, $a=0$, $-a$ положителен.*

X. *Сумма и произведение положительных элементов положительны.*

Условия I — X означают, что D — расположенное поле. Стало быть, определяя $a>b$, если элемент $a-b$ положителен, превратим D в упорядоченное множество (§ 10, теорема 1). Далее:

XI. (Аксиома Архимеда.) *Для любых элементов a и b множества D, где $b>0$, существует натуральное число n такое, что $nb>a$.*

Условия I — XI означают, что D — архимедовски расположенное поле. Стало быть, в D определены понятия предела последовательности и фундаментальной последовательности, не меняющиеся при замене D любым его подполем, содержащим все рассматриваемые элементы (§ 24, теорема 5). Наконец:

XII. (Аксиома полноты.) *Любая фундаментальная последовательность элементов множества D имеет предел в этом множестве.*

Условия I — XII означают, что D — непрерывное поле (§ 24, определение 6).

Отметим, что это определение предполагает уже построенные натуральные числа. Иначе аксиома Архимеда XI теряет смысл. Ниже мы приведём другую систему аксиом, не опирающуюся на понятие натурального числа.

Возникает вопрос о непротиворечивости, полноте и независимости системы аксиом I — XII.

Для доказательства непротиворечивости системы аксиом I—XII достаточно найти для неё хотя бы одну интерпретацию (§ 17, определение 1). Но поле D_0, построенное в § 25 (определение 2, теорема 4), даёт такую интерпретацию. Правда, построение поля D_0 опирается на поле рациональных чисел, но, беря конструктивное определение его, т. е. поле Γ_0 (§ 22, определение 2), где за кольцо целых чисел принято его конструктивное определение C_0 (§ 20, определение 2), мы сводим построение поля D_0 к натуральным числам. Этим непротиворечивость системы аксиом I—XII сведена к непротиворечивости (в смысле существования интерпретации) системы аксиом для натуральных чисел.

Для доказательства полноты системы аксиом I—XII достаточно показать, что две любые интерпретации этой системы изоморфны (§ 17, определение 3). Но это, по сути дела, нами уже доказано.

В самом деле, если P_1 и P_2 — две интерпретации системы аксиом I—XII (т. е. два непрерывных поля), то для одной и той же интерпретации Γ поля рациональных чисел существуют поля D_1 и D_2, содержащие в качестве подполя поле Γ и изоморфные (относительно сложения, умножения и расположения) соответственно P_1 и P_2 (§ 23, теорема 2). В силу этого изоморфизма поля D_1 и D_2 сами непрерывны и, следовательно, изоморфны относительно обеих операций и порядка (§ 25, теорема 2). Но тогда по свойствам изоморфизма поля P_1 и P_2 изоморфны между собой (также относительно сложения, умножения и расположения).

Этим полнота системы аксиом I—XII доказана.

Поскольку непротиворечивость и полнота системы аксиом I — XII доказаны, эта система точно определяет поле действительных чисел и является фундаментом для построения теории действительного числа. Такое построение было в известных пределах выполнено нами в предыдущем параграфе.

Вопрос о независимости системы аксиом I — XII (§ 17, определение 3) не имеет такого принципиального значения, и мы им заниматься не будем. Укажем лишь, что каждая из аксиом XI и XII независима от остальных аксиом I—XII.

Мы определили непрерывность расположенного поля при помощи аксиомы Архимеда и аксиомы полноты (§ 24, определение 6). Существует много других форм аксиом непрерывности. Приведём две из них. Чтобы их формулировать, нужно ввести некоторые новые понятия.

Сечением упорядоченного множества (и, в частности, расположенного поля) P называется пара непустых подмножеств X, Y множества P, не имеющих общих элементов, объединение которых (§ 2) равно P, т. е.

$$X \cap Y = 0, \quad X \cup Y = P,$$

причём $x < y$ для любых элементов $x \in X$ и $y \in Y$. Если элемент a является наибольшим элементом в X, причём Y не имеет наименьшего элемента или же a является наименьшим элементом Y, причём X не имеет наибольшего элемента, то элемент a называется *рубежом данного сечения*.

Элемент b упорядоченного множества P называется *предельным элементом множества* A, если для любых элементов b_1 и b_2 таких, что $b_1 < b < b_2$, существует бесконечное множество элементов a из A, для которых $b_1 < a < b_2$.

Легко убедиться, что для расположенного поля P это определение эквивалентно такому:

Элемент b называется *предельным для множества* A, если для любого элемента $\varepsilon > 0$ из P существует бесконечное множество элементов a из A, для которых $|a - b| < \varepsilon$.

Подмножество A упорядоченного множества (и, в частности, расположенного поля) P называется *ограниченным*, если существуют элементы b_1 и b_2 из P такие, что $b_1 < a < b_2$ для любого элемента a множества A.

Следующие три свойства расположенного поля P эквивалентны.

а) *В поле P выполнены аксиомы* XI *и* XII.

б) (Дедекинд). *Любое сечение поля P имеет рубеж.*

в) (Вейерштрасс). *Любое бесконечное ограниченное множество элементов поля P имеет предельный элемент.*

Таким образом, поле действительных чисел аксиоматически можно определить свойствами I — X и любым из свойств а), б), в). Доказательство эквивалентности свойств а), б), в) можно найти в книге И. В. Проскурякова [5].

Поле рациональных чисел аксиоматически можно определить как простое поле характеристики нуль. В самом деле, любое такое поле совпадает со своим подполем рациональных элементов и, следовательно, изоморфно полю рациональных чисел Г (§ 23, теорема 2).

Кольцо целых чисел аксиоматически можно определить, как кольцо R с единицей e, не содержащее отличного от него подкольца с единицей и обладающее тем свойством, что $ne \neq 0$ для любого натурального числа n. В самом деле, легко показать, что множество всех элементов вида ne изоморфно множеству N натуральных чисел относительно сложения и умножения. Следовательно, кольцо R содержит подкольцо R_0, изоморфное кольцу целых чисел C (§ 20, теорема 3). Но так как R_0 содержит единицу, то оно совпадает с R. Таким образом, R изоморфно кольцу целых чисел.

ГЛАВА VII

ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

§ 28. Определение поля комплексных чисел

Уже в древности при решении задач, выражаемых на современном языке квадратными уравнениями, встречались случаи, связанные с комплексными корнями уравнений. В таких случаях считали задачу неразрешимой. Однако решение в радикалах кубичного уравнения, найденное итальянскими математиками в первой половине XVI в., приводило к выражению действительных корней уравнения с действительными коэффициентами через квадратные корни из отрицательных чисел. Это заставило математиков того времени оперировать новыми числами, которые назывались «мнимыми», «невозможными», «воображаемыми» и т. д., применяя для них те же правила действий, которым подчинялись действительные числа. Однако смысл новых чисел оставался неясным, что и нашло своё отражение в терминологии. Так, Кардан называет новые числа «ложными, поистине софистическими» числами. Первое формальное обоснование действий с комплексными числами дано в «алгебре» итальянского математика Бомбелли (1572). Однако наглядное геометрическое изображение этих чисел (как точек или векторов на плоскости) было дано только в начале XIX в. [1]).

После этого изучение комплексных чисел пошло очень быстро, и в настоящее время теория функций комплексного переменного является основной частью математического анализа. Эта теория находит приложение в самых разнообразных областях науки, например в аэродинамике. Свойства комплексных чисел столь же хорошо обоснованы как, скажем, свойства чисел рациональных или действительных.

В поле действительных чисел операция извлечения корня не всегда выполнима. Именно, корень чётной степени из отрицатель-

[1]) Впервые геометрическое изображение действий над комплексными числами было дано датским землемером К. Бесселем в 1799 г. и независимо от него французским математиком Аргандом в 1806 г. Однако общее признание оно получило лишь после нового обоснования, данного Гауссом в 1831 г.

ного числа не имеет действительных значений, т. е. при действительном $a<0$ и чётном натуральном n не существует действительного b, для которого $b^n=a$ (§ 26, теорема 4). Следуя общему плану расширения числовых областей, намеченному в § 18, мы расширим теперь поле действительных чисел D до поля комплексных чисел K, в котором операция извлечения корня уже всегда выполнима. При этом получается существенно новый результат и для тех случаев, когда эта операция была выполнима в поле D. Именно, в новом поле K $\sqrt[n]{a}$ при любом $a\neq 0$ и любом натуральном n будет иметь ровно n значений [1]).

Как мы увидим, достаточно расширить поле D до такого поля, где $\sqrt{-1}$ имеет хотя бы одно значение, т. е. существует элемент i, для которого $i^2=-1$. Мы будем искать минимальное расширение такого рода в смысле следующего определения:

Определение 1. *Полем комплексных чисел называется минимальное поле K, содержащее поле действительных чисел D и элемент i со свойством $i^2=-1$, т. е. множество K, обладающее следующими свойствами*:

1) *K является полем, содержащим в качестве подполя поле действительных чисел D и элемент i со свойством $i^2=-1$.*

2) *Поле K не содержит никакого подполя, отличного от него самого и обладающего теми же свойствами. Элементы поля K называются комплексными числами.*

Сначала докажем единственность (как всегда, с точностью до изоморфизма) определённого таким образом поля K.

Теорема 1. *Поле K, содержащее поле действительных чисел D [2]) и элемент i со свойством $i^2=-1$, будет минимальным* (т. е. *полем комплексных чисел*) *тогда и только тогда, когда каждый элемент x из K можно представить в виде*

$$x=a+bi, \tag{1}$$

где a и b — действительные числа. При этом такое представление единственно, т. е. для данного элемента x из K существует лишь одна пара действительных чисел a, b (взятых в данном порядке), *удовлетворяющих равенству* (1).

---

[1]) Значения $\sqrt[n]{a}$ являются, очевидно, корнями уравнения $x^n-a=0$. Уравнения такого вида называются *двучленными*. Таким образом, в поле комплексных чисел K разрешимы все двучленные уравнения. Справедливо более сильное утверждение, что в поле K разрешимы все алгебраические уравнения, т. е. уравнения вида $f(x)=0$, где $f(x)$ — любой многочлен степени $n\geqslant 1$ с любыми комплексными коэффициентами. Доказательство этой теоремы см. Э. э. м., книга 2, Л. Я. Окунев, кольцо многочленов и поле рациональных функций, гл. I, § 6.

[2]) Как всегда, говоря, что одно поле содержит другое, мы подразумеваем, что операции в меньшем поле совпадают с одноимёнными операциями в большем поле.

Доказательство. а) Пусть каждый элемент x поля K представим в виде (1) с действительными a и b и пусть P — любое подполе поля K, содержащее поле действительных чисел D и некоторый элемент j со свойством $j^2=-1$. Так как $i^2=j^2=-1$, то $(i+j)(i-j)=i^2-ij+ji-j^2=0$. Но поле K не имеет делителей нуля (§ 8, теорема 1), следовательно, либо $i+j=0$, либо $i-j=0$, откуда $j=\pm i$. Для любого x из K тогда $x=a+bi=a\pm bj$, т. е. x принадлежит P, P совпадает с K. Этим доказана минимальность поля R.

б) Пусть, обратно, поле K минимально. Покажем, что любой элемент x из K представим в виде (1). Пусть M есть множество всех элементов поля K, представимых в виде (1). Покажем, что выполняются следующие свойства:

$$\left.\begin{array}{ll} \text{а)} & a+bi=c+di \\ & \text{тогда и только тогда, когда } a=c \text{ и } b=d; \\ \text{б)} & (a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i; \\ \text{в)} & (a+bi)(c+di)=(ac-bd)+(ad+bc)i; \\ \text{г)} & \dfrac{a+bi}{c+di}=\dfrac{ac+bd}{c^2+d^2}+\dfrac{bc-ad}{c^2+d^2}i, \\ & \text{где } c+di\neq 0. \end{array}\right\} \quad (2)$$

В самом деле, если $a=c$ и $b=d$, то из однозначности суммы и произведения в поле K следует, что $a+bi=c+di$. Обратно, если $a+bi=c+di$, то из $b=d$ следует $bi=di$, а потому $a=c$. Если же $b\neq d$, то $i=\dfrac{a-b}{d-c}$, т. е. i принадлежит полю действительных чисел, что невозможно, ибо $i^2=-1<0$, а квадрат действительного числа не отрицателен (§ 10, теорема 7). Таким образом, $b=d$ и $a=c$, чем доказано утверждение а).

Так как из свойств нуля очевидно, что $0+0\cdot i=0$, то из а), в частности, следует, что $a+bi=0$ тогда и только тогда, когда $a=b=0$.

Равенства б) и в) следуют непосредственно из свойств сложения и умножения в поле K.

Если $c+di\neq 0$, то либо $c\neq 0$, либо $d\neq 0$ и по доказанному выше также $c-di\neq 0$. В этом случае также $c^2+d^2>0$. Умножая делимое и делитель в левой части равенства г) на $c-di\neq 0$, мы не изменим частного и легко приведём его к выражению, стоящему в правой части равенства.

Из а) следует однозначность представления элемента x в виде (1).

Из б), в) и г) следует, что сумма, разность, произведение и частное (если делитель отличен от нуля) двух элементов множества M снова принадлежат M, т. е. M есть подполе поля P (§ 8,

теорема 5). Так как $a = a + 0 \cdot i$ и $i = 0 + 1i$ принадлежат M и K — минимально, то $K = M$, т. е. любой элемент из K представим в виде (1).

Теорема 2. *Все поля комплексных чисел изоморфны между собой, т. е. поле комплексных чисел определено однозначно с точностью до изоморфизма.*

Доказательство. Пусть K_1 и K_2 — два поля комплексных чисел, причём K_1 содержит элемент i_1, а K_2 — элемент i_2 со свойством $i_1^2 = i_2^2 = -1$. По предыдущей теореме все элементы K_1 записываются в виде $a + bi_1$ и все элементы из K_2 — в виде $a + bi_2$ с действительными a и b, причём однозначно. Отсюда легко вывести, что соответствие $f(a + bi_1) = a + bi_2$ является взаимно однозначным отображением K_1 на K_2. Из равенств (2), б), в) следует, что сложение и умножение элементов из K_1 и K_2 сводится к одним и тем же действиям над действительными числами. Отсюда легко вывести, что отображение f изоморфно. Надо доказать, что

$$f(x_1 + y_1) = f(x_1) + f(y_1), \quad f(x_1 y_1) = f(x_1) f(y_1)$$

для любых x_1 и y_1 из K_1. Проверим лишь первое из этих соотношений, так как для второго рассуждение аналогично.

Пусть $x_1 = a + bi_1$, $y_1 = c + di_1$. Тогда

$$f(x_1) = a + bi_2, \quad f(y_1) = c + di_2,$$

$$f(x_1 + y_1) = f[(a + bi_1) + (c + di_1)] = f[(a + c) + (b + d)i_1] =$$
$$= (a + c) + (b + d)i_2 = (a + bi_2) + (c + di_2) = f(x_1) + f(y_1).$$

Теорема доказана.

Замечание. При изоморфизме f любое действительное число a отображается само на себя, а элемент i_1 переходит в i_2.

Теорема 3. *Любое поле P, содержащее поле действительных чисел D и элемент i со свойством $i^2 = -1$, содержит поле комплексных чисел.*

Доказательство. Пусть K — множество всех элементов поля P, представимых в виде $a + bi$ с действительными a и b.

Как в доказательстве теоремы 1 [п. б)], убеждаемся, что K — подполе поля P; K содержит поле действительных чисел D и элемент i. Так как любой элемент из K имеет вид $a + bi$, то по теореме 1 поле K минимально в смысле определения 1, т. е. K является полем комплексных чисел. Теорема доказана.

Теперь докажем существование поля комплексных чисел. Как и в случае целых рациональных и действительных чисел, достаточно построить интерпретацию (конкретный пример) поля, удовлетворяющего определению 1. Можно было бы элементами этого поля просто считать символы $a + bi$, где a и b — действительные числа, а i — символ, подчинённый условию $i^2 = -1$. Но тогда надо показать,

что в это поле можно включить действительные числа так, что символ $a+bi$ в новом поле будет совпадать с суммой a и произведения b на i. Такое построение ввиду неясности смысла, придаваемого символу i, может показаться слишком формальным. Поэтому мы поступим несколько иначе. По идее, приведённой ниже, построение очень близко к упомянутому выше, но все применяемые в нём символы имеют вполне конкретный смысл.

Конструкция одного из изоморфных полей комплексных чисел подсказывается теоремой 1. В самом деле, каждый элемент искомого поля должен иметь вид $a+bi$, т. е. определяется парой действительных чисел a, b, причём разным парам соответствуют и разные элементы. Таким образом, в данном случае нам не нужно определять эквивалентность пар и переходить к классам эквивалентных пар, как в случае целых или рациональных чисел.

Определение 2. *Пусть K_0 есть множество всех пар вида (a, b), где a и b — действительные числа, порядок которых существенен. Сложение и умножение во множестве K_0 определяем по формулам*

$$(a, b)+(c, d)=(a+c, b+d), \tag{3}$$

$$(a, b)(c, d)=(ac-bd, ad+bc). \tag{4}$$

Операции в K_0 определены так, чтобы им соответствовали те же операции в искомом поле, которые должны удовлетворять равенствам (2), б), в).

Теорема 4. *Множество K_0 с операциями, определёнными по формулам* (3) *и* (4), *является полем.*

Доказательство. Надо проверить выполнение в K_0 свойств I — VIII (§ 7, определение 1 и § 8, определение 1).

Так как сложение пар сводится к сложению соответствующих элементов, то свойства I — III для пар непосредственно вытекают из соответствующих свойств действительных чисел.

Свойства IV — VI проверяются непосредственно. Проверим, например, дистрибутивность умножения относительно сложения (свойство VI):

$$\begin{aligned}[(a, b)+(c, d)](e, f)&=(a+c, b+d)(e, f)=\\&=[(a+c)e-(b+d)f, (a+c)f+(b+d)e]=\\&=(ae+ce-bf-df, af+cf+be+df);\end{aligned}$$

$$\begin{aligned}(a, b)(c, f)+(c, d)(e, f)&=(ae-bf, af+be)+(ce-df, cf+de)=\\&=(ae-bf+ce-df, af+be+cf+de).\end{aligned}$$

Обе окончательно полученные пары совпадают, чем и доказано VI.

Итак, K_0 является кольцом. Легко видеть, что нулём этого кольца является пара (0, 0), а противоположная пара и разность пар определяются равенствами

$$-(a, b)=(-a, -b),\ (a, b)-(c, d)=(a-c, b-d).$$

Проверяем обратимость умножения (свойство VII). Пусть (a, b) и (c, d) — две любые пары, причём $(a, b)\neq(0, 0)$. Последнее означает, что либо $a\neq 0$, либо $b\neq 0$ [1]).

Так как a и b — действительные числа, то $a^2+b^2>0$ (§ 10, теорема 7). Надо найти пару (x, y), удовлетворяющую уравнению

$$(a, b)(x, y)=(c, d). \tag{5}$$

Предположим сначала, что такая пара существует. Тогда

$$(ax-by,\ ay+bx)=(c, d),$$

откуда $ax-by=c$, $bx+ay=d$. Решая эту систему уравнений относительно x и y, найдём:

$$x=\frac{ac+bd}{a^2+b^2},\quad y=\frac{ad-bc}{a^2+b^2}.$$

Этим доказано, что если пара (x, y), удовлетворяющая (5), существует, то только одна, именно та, где x и y определяются из написанных для них выражений. Легко проверить, что такая пара действительно удовлетворяет равенству (5). В самом деле,

$$(a, b)\left(\frac{ac+bd}{a^2+b^2},\ \frac{ad-bc}{a^2+b^2}\right)=$$
$$=\left(\frac{a^2c+abd-bad+b^2c}{a^2+b^2},\ \frac{a^2d-abc+bac+b^2d}{a^2+b^2}\right)=(c, d).$$

Этим свойство VII доказано.

Так как K_0 содержит более одного элемента, то свойство VIII выполнено. Теорема доказана.

Отметим, что единицей поля K_0 является пара (1, 0), так как $(a, b)\cdot(1, 0)=(a\cdot 1-b\cdot 0,\ a\cdot 0+b\cdot 1)=(a, b)$.

Мы увидим, что поле K_0 с точностью до изоморфизма является полем комплексных чисел. Это поле не удовлетворяет определению 1, ибо оно не содержит действительных чисел.

Займёмся включением в поле K_0 поля действительных чисел D. Пусть D' — множество всех пар поля K_0 вида $(a, 0)$. Из формул (3) и (4), определяющих сложение и умножение пар, легко следует, что отображение $a\to(a, 0)$ является изоморфным отображением поля D на множество D'. Следовательно, D' само является полем (§ 9, теорема 1). Далее, существует поле K, содержащее D в ка-

[1]) Равенство и неравенство пар, как и элементов любых множеств, мы понимаем просто как тождество или различие. Таким образом $(x, y)=(z, t)$ тогда и только тогда, когда $x=z$, $y=t$.

честве подполя и отображающееся на K_0 изоморфно так, что каждое число a из D отображается при этом на соответствующую ему пару $(a, 0)$ из D' (§ 9, теорема 2):

Теорема 5. *Поле K является полем комплексных чисел.*

Доказательство. По построению поле K содержит поле D. Далее, поле K содержит пару $(0, 1)$. Обозначим эту пару через i, т. е. положим: $i=(0, 1)$. В поле K_0 мы имеем:

$$(0, 1)^2=(0, 1)(0, 1)=(0\cdot 0-1\cdot 1,\ 0\cdot 1+1\cdot 0)=(-1, 0).$$

Но при построенном выше изоморфном отображении K_0 на K элементу $(-1, 0)$ из K_0 соответствует число -1 из K. Следовательно, в K должно быть $i^2=-1$. Итак, поле K обладает свойством 1) из определения 1.

Остаётся доказать минимальность поля K. По теореме 1 для этого достаточно показать, что любой элемент x из K представим в виде $x=a+bi$ с действительными a и b. Пусть при упомянутом изоморфизме K и K_0 элементу x из K соответствует пара (a, b) из K_0. Легко проверить справедливость равенства

$$(a, b)=(a, 0)+(b, 0)(0, 1)$$

в K_0. Отсюда в силу нашего изоморфизма между K_0 и K находим: $x=a+bi$. Теорема доказана.

§ 29. Свойства комплексных чисел [1])

Поле комплексных чисел обладает всеми свойствами колец и полей, рассмотренными в §§ 7, 8.

Так как поле комплексных чисел содержит поле рациональных чисел, то его характеристика равна нулю.

Так как в любом расположенном поле $a^2\geqslant 0$ для любого элемента a (§ 10, теорема 7), а в поле комплексных чисел $i^2=-1$, то поле комплексных чисел не может быть расположено.

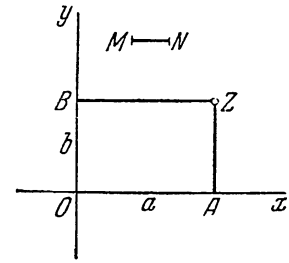


Рис. 2.

Геометрическое представление комплексных чисел. Возьмём на плоскости две взаимно перпендикулярные прямые — горизонтальную Ox и вертикальную Oy, — пересекающиеся в точке O (рис. 2). Далее, выберем некоторый отрезок MN за единицу измерения отрезков. Тогда все

[1]) Здесь мы остановимся лишь на обосновании элементарных свойств комплексных чисел. Читателю, желающему ознакомиться с другими интересными свойствами этих чисел (например, с теорией делимости так называемых целых комплексных чисел), рекомендуем книгу Р. О. Кузьмина и Д. К. Фаддеева [13].

комплексные числа можно изобразить точками плоскости Oxy. Именно, для числа $z=a+bi$ откладываем на Ox от точки O отрезок OA длины $|a|$ и притом вправо, если $a>0$, и влево, если $a<0$. На прямой Oy откладываем отрезок OB длины $|b|$ и притом вверх, если $b>0$, и вниз, если $b<0$. Через точку A проводим прямую, параллельную Oy, а через B — прямую, параллельную Ox. Точка Z пересечения этих прямых и принимается за изображение числа z. Легко убедиться, что любая точка нашей плоскости является изображением некоторого комплексного числа и что данное соответствие между комплексными числами и точками плоскости Oxy взаимно однозначно. Очевидно, что при этом число $z=a+bi$ изображается точкой $Z(a, b)$ с прямоугольными декартовыми координатами a и b.

Действительные числа и только они изображаются точками прямой Ox. Числа вида bi, называемые *чисто мнимыми*, и только они изображаются точками прямой Oy. Поэтому прямая Ox называется *действительной*, а Oy — *мнимой осью*. Направления вправо по Ox и вверх по Oy называются *положительными*, а влево по Ox и вниз по Oy — *отрицательными*. Точка O называется *началом координат*, а прямые Ox и Oy — *осями координат*.

Во всём дальнейшем мы не будем непосредственно опираться на геометрическое представление комплексных чисел для доказательства каких-либо их свойств; мы будем, однако, прибегать к геометрическому представлению для придания наглядности этим свойствам.

Тригонометрическая форма комплесного числа.

Определение. *Тригонометрической формой комплексного числа z называется его запись в виде*

$$z=r(\cos\alpha+i\sin\alpha),$$

где r и α — числа действительные, причём $r\geqslant 0$. Число r называется модулем, а α — аргументом комплексного числа z.

Теорема 1. *Любое комплексное число можно записать в тригонометрической форме. При этом модуль z определён однозначно и равен нулю тогда и только тогда, когда $z=0$, а аргумент для $z=0$ может быть произвольным числом, а для $z\neq 0$ определён с точностью до слагаемого, кратного 2π.*

Доказательство. Если $z=0$, то $0\cdot(\cos\alpha+i\sin\alpha)$ при любом α будет тригонометрической формой числа z. Обратно, если $r(\cos\alpha+i\sin\alpha)=0$, то из $\sin^2\alpha+\cos^2\alpha=1$ следует, что $\cos\alpha+i\sin\alpha\neq 0$ и, следовательно, $r=0$. Этим все утверждения теоремы, касающиеся случая $z=0$, доказаны.

Пусть $z=a+bi\neq 0$. Тогда числа a и b не равны нулю одновременно и $a^2+b^2>0$. В поле действительных чисел $\sqrt{a^2+b^2}$ имеет два значения: положительное и отрицательное (§ 26, теорема 4). Пусть r — положительное значение этого корня. Так как $a^2\leqslant r^2$ и

$b^2 \leqslant r^2$, то $\left|\frac{a}{r}\right| \leqslant 1$ и $\left|\frac{b}{r}\right| \leqslant 1$. Существует число α_0 такое, что $0 \leqslant \alpha_0 \leqslant \frac{\pi}{2}$ и $\sin \alpha_0 = \left|\frac{b}{r}\right|$ (§ 26, теорема 5). Так как $\left(\frac{a}{r}\right)^2 + \left(\frac{b}{r}\right)^2 = 1$, то $\frac{a}{r} = \pm \cos \alpha_0$ и $\frac{b}{r} = \pm \sin \alpha_0$.

Если $\frac{a}{r} = \cos \alpha_0$ и $\frac{b}{r} = \sin \alpha_0$, то положим $\alpha = \alpha_0$; если $\frac{a}{r} = -\cos \alpha_0$ и $\frac{b}{r} = \sin \alpha_0$, то положим: $\alpha_0 = \pi - \alpha_1$ и $\alpha = \alpha_1$; если $\frac{b}{r} = -\sin \alpha_1$, то положим: $\alpha_1 = -\alpha$. Всегда получим число α такое, что

$$\frac{a}{r} = \cos \alpha, \quad \frac{b}{r} = \sin \alpha,$$

и таким образом

$$z = a + bi = r\left(\frac{a}{r} + i\frac{b}{r}\right) = r(\cos \alpha + i \sin \alpha).$$

Итак, z записано в тригонометрической форме. Очевидно, что, прибавляя к α число $2k\pi$ с любым целым k, мы получим тригонометрическую форму того же числа z.

Докажем единственность модуля. Пусть $a + bi = r(\cos \alpha + i \sin \alpha)$. Тогда

$$a = r \cos \alpha, \quad b = r \sin \alpha. \tag{1}$$

Возводя эти равенства в квадрат и складывая, находим: $a^2 + b^2 = r^2$, т. е. $r = \sqrt{a^2 + b^2}$. Мы берём положительное значение корня, ибо $r > 0$. Этим единственность r доказана.

Наконец, если даны две тригонометрические формы числа z:

$$r(\cos \alpha_1 + i \sin \alpha_1) = r(\cos \alpha_2 + i \sin \alpha_2),$$

то при $z \neq 0$ также $r \neq 0$, откуда

$$\cos \alpha_1 = \cos \alpha_2, \quad \sin \alpha_1 = \sin \alpha_2$$

и, как известно из тригонометрии, тогда $\alpha_1 = \alpha_2 + 2k\pi$ с целым k. Теорема доказана.

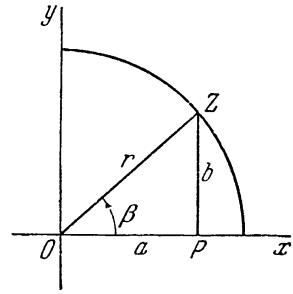


Рис. 3.

Выясним геометрический смысл модуля и аргумента. Пусть числу $z = r(\cos \alpha + i \sin \alpha)$ соответствует точка Z плоскости Oxy (рис. 3). Соединим эту точку отрезком прямой с началом координат O и опустим из точки Z на действительную ось Ox перпендикуляр ZP. Если $z = a + bi$, то длина отрезка OP равна $|a|$, а длина ZP равна $|b|$. Поэтому

$$OZ^2 = OP^2 + ZP^2 = a^2 + b^2 = r^2,$$

откуда $r = OZ$. Итак, модуль числа z равен расстоянию точки Z от

начала координат. Если β — радианная мера угла, образуемого лучом OZ с положительным направлением действительной оси, отсчитываемого от нее в направлении, совпадающем с кратчайшим поворотом от положительного направления действительной до положительного направления мнимой оси, то, проведя окружность радиуса r с центром O, мы видим, что a и b по абсолютной величине и по знаку совпадают с линией косинуса и линией синуса угла β. Таким образом, в силу (1) должно быть:

$$\cos\beta = \frac{a}{r} = \cos\alpha, \quad \sin\beta = \frac{b}{r} = \sin\alpha,$$

откуда $\alpha = \beta + 2k\pi$. Итак, аргумент числа z с точностью до слагаемого, кратного 2π, равен углу луча OZ с положительным направлением действительной оси.

Из доказанного вытекает, что модуль и аргумент числа z являются полярными координатами соответствующей точки Z в системе полярных координат, у которой полюс лежит в начале координат O, а полярная ось совпадает с положительным направлением действительной оси Ox.

Умножение комплексных чисел, заданных в тригонометрической форме, выглядит особенно просто.

Теорема 2. *При умножении любого конечного числа комплексных чисел модули их перемножаются, а аргументы складываются.*

Доказательство. Ограничимся случаем двух сомножителей, так как проведение индукции не представляет затруднений. Итак, надо доказать:

$$[r_1(\cos\alpha_1 + i\sin\alpha_1)] \cdot [r_2(\cos\alpha_2 + i\sin\alpha_2)] = \\ = (r_1 r_2)[\cos(\alpha_1 + \alpha_2) + i\sin(\alpha_1 + \alpha_2)]. \quad (2)$$

Но

$$(\cos\alpha_1 + i\sin\alpha_1)(\cos\alpha_2 + i\sin\alpha_2) = (\cos\alpha_1\cos\alpha_2 - \sin\alpha_1\sin\alpha_2) + \\ + i(\cos\alpha_1\sin\alpha_2 + \sin\alpha_1\cos\alpha_2) = \cos(\alpha_1 + \alpha_2) + i\sin(\alpha_1 + \alpha_2).$$

Отсюда непосредственно вытекает (2). Так как из $r_1 \geqslant 0$, $r_2 \geqslant 0$ следует $r_1 r_2 \geqslant 0$, то $r_1 r_2$ — модуль и $\alpha_1 + \alpha_2$ — аргумент произведения данных чисел, чем теорема для случаев двух сомножителей доказана.

Из этой теоремы вытекает

Теорема 3. *При делении комплексных чисел модули делятся, а аргументы вычитаются, точнее*

$$\frac{r_1(\cos\alpha_1 + i\sin\alpha_1)}{r_2(\cos\alpha_2 + i\sin\alpha_2)} = \frac{r_1}{r_2}[\cos(\alpha_1 - \alpha_2) + i\sin(\alpha_1 - \alpha_2)]. \quad (3)$$

Доказательство. Частное, как и любое комплексное число, можно записать в тригонометрической форме. Пусть эта запись будет: $r_0(\cos\alpha_0 + i\sin\alpha_0)$. По определению частного тогда

$$r_1(\cos\alpha_1 + i\sin\alpha_1) = r_2(\cos\alpha_2 + i\sin\alpha_2)\cdot r_0(\cos\alpha_0 + i\sin\alpha_0) = \\ = r_2 r_0[\cos(\alpha_2 + \alpha_0) + i\sin(\alpha_2 + \alpha_0)],$$

откуда, включая в α_0 слагаемое, кратное 2π, находим: $r_1 = r_2 r_0$, $\alpha_1 = \alpha_2 + \alpha_0$, т. е. $r_0 = \frac{r_1}{r_2}$, $\alpha_0 = \alpha_1 - \alpha_2$, чем теорема доказана.

При совпадении сомножителей из теоремы 2 получается так называемая *формула Муавра*

$$[r(\cos\alpha + i\sin\alpha)]^n = r^n(\cos n\alpha + i\sin n\alpha). \qquad (4)$$

Теперь легко решается вопрос об извлечении корня из комплексного числа.

Теорема 4. *Пусть z — комплексное и n — натуральное число. В поле комплексных чисел $\sqrt[n]{z}$ имеет при $z = 0$ единственное значение* 0, *а при $z \neq 0$* имеет *n различных значений. Если*

$$z = r(\cos\alpha + i\sin\alpha),$$

то эти значения находятся по формуле

$$z_k = \sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right) \quad (k = 0,\ 1,\ 2,\ \ldots,\ n-1). \qquad (5)$$

Доказательство. $0^n = 0$ и из $x^n = 0$ в силу отсутствия делителей нуля в поле K (§ 8, теорема 1) следует $x = 0$. Таким образом, при $z = 0$ единственное значение $\sqrt[n]{z}$ есть 0.

Пусть

$$z = r(\cos\alpha + i\sin\alpha) \neq 0.$$

Тогда $r \neq 0$ и аргумент α определён с точностью до кратного 2π.

Предположим, что $\sqrt[n]{z}$ имеет значение x в поле комплексных чисел. Это означает, что $x^n = z$. По теореме 1 число x можно записать в тригонометрической форме:

$$x = r'(\cos\alpha' + i\sin\alpha'), \quad r' > 0.$$

Тогда по формуле Муавра (4) находим:

$$r'^n(\cos n\alpha' + i\sin n\alpha') = r(\cos\alpha + i\sin\alpha),$$

откуда

$$r'^n = r, \quad n\alpha' = \alpha + 2k\pi, \quad r' = \sqrt[n]{r}, \quad \alpha' = \frac{\alpha + 2k\pi}{n}.$$

Можно считать, что целое число k удовлетворяет условию $0 \leqslant k \leqslant n-1$. В самом деле, деля k на n, находим: $k = nq + k_1$, где q и k_1 — целые числа и $0 \leqslant k_1 \leqslant n-1$. Тогда

$$\alpha' = \frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2k_1\pi}{n} + 2q\pi;$$

но так как аргумент числа x определён лишь с точностью до кратного от 2π, то можно считать, что он равен $\frac{\alpha + 2k_1\pi}{n}$.

Итак,

$$x = \sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right) \quad (0 \leqslant k \leqslant n-1).$$

Мы доказали, что если существует значение $\sqrt[n]{z}$, то оно совпадает с одним из n чисел z_k, определяемых равенством (5).

Легко показать, что все числа z_k, определяемые из (5), действительно являются значениями $\sqrt[n]{z}$ и притом даже при любом целом k. В самом деле,

$$z_k^n = (\sqrt[n]{r})^n\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right) = r(\cos\alpha + i\sin\alpha) = z.$$

Наконец, покажем, что все n чисел z_k при $k = 0, 1, 2, \ldots, n-1$ различны между собой. Если $k \neq l$, то по теореме 1 из $r \neq 0$ и $z_k = z_l$ следует

$$\frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2l\pi}{n} + 2m\pi$$

с целым m, откуда $k - l = mn$. Но из $0 \leqslant k < n$ и $0 \leqslant l < n$ следует $|k - l| < n$, т. е. $|mn| < n$, $|m| < 1$, и так как m — целое, то $m = 0$, $k = l$, что невозможно. Теорема доказана.

Из равенств (5) ясно, какой геометрический смысл имеют значения $\sqrt[n]{z}$ при $z \neq 0$. Так как модуль у всех чисел z_k общий, то точки, изображающие эти числа, лежат на окружности радиуса $\sqrt[n]{r}$ с центром в начале координат. Аргументы соседних чисел z_k и z_{k+1} отличаются на $\frac{2\pi}{n}$, и следовательно, точки, изображающие числа z_k, лежат в вершинах правильного n-угольника, вписанного в упомянутую окружность, причём одна из вершин изображает число z_0 с аргументом $\frac{\alpha}{n}$, чем однозначно определяется положение остальных вершин.

После выяснения геометрического смысла значений $\sqrt[n]{z}$ полученные прежде (§ 26, теорема 4) свойства корней из действительных чисел получают наглядное истолкование.

Пусть надо найти действительные значения $\sqrt[n]{z}$ из действительного числа $z \neq 0$. Эти значения изобразятся вершинами указанного выше правильного n-угольника, лежащими на действительной оси. Отсюда сразу ясно, что действительных значений может быть не более двух, и если их два, то они равны по абсолютной величине и противоположны по знаку. Если $z > 0$, то его аргумент $\alpha = 0$ и вершина, изображающая число z_0, лежит на положительной действительной полуоси. При чётном n противоположная вершина также попадает на действительную ось, и мы получим два действительных значения корня; при нечётном же n другая вершина не может попасть на действительную ось, и мы получаем одно действительное значение. Если $z < 0$, то $\alpha = \pi$. Число z_k будет действительным, если его аргумент кратен π. При нечётном n аргумент $\frac{\pi + 2k\pi}{n} = \pi \frac{2k+1}{n}$ будет кратен π при $k = \frac{n-1}{2}$, и мы получим одно действительное значение корня с аргументом π, т. е. отрицательное, а при чётном n аргумент $\pi \frac{2k+1}{n}$ не может быть кратным π, и мы вовсе не получим действительных значений корня.

Свойства модуля. Модуль комплексного числа z обозначается через $|z|$. Совпадение этого обозначения с обозначением абсолютной величины в случае действительного z не ведёт к противоречию, ибо если $z = a + bi$ — действительное число, то $b = 0$, и для модуля z находим:

$$|z| = \sqrt{a^2 + b^2} = \sqrt{a^2} = |a|,$$

т. е. модуль действительного числа совпадает с его абсолютной величиной.

Комплексные числа

$$z = a + bi \quad \text{и} \quad \bar{z} = a - bi$$

называются *сопряжёнными*. Очевидно, что сопряжённые числа имеют одинаковый модуль. Далее, произведение сопряжённых чисел равно квадрату их модуля:

$$z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 = r^2.$$

Отсюда

$$|z| = \sqrt{z\bar{z}}. \tag{6}$$

Модуль комплексного числа обладает свойствами, аналогичными свойствам абсолютной величины элемента расположенного поля (§ 10, теорема 8), а именно:

$$|xy| = |x| \cdot |y|, \tag{7}$$

$$|x + y| \leqslant |x| + |y| \tag{8}$$

для любых комплексных чисел x и y.

В самом деле, равенство (7) содержится в теореме 2. Если же не использовать тригонометрическую форму чисел, а принять за определение модуля $|z|$ равенство (6), то (7) можно доказать так:

$$|xy|=\sqrt{(xy)\,(\overline{xy})}=\sqrt{xy\,\bar{x}\,\bar{y}}=\sqrt{x\bar{x}}\,\sqrt{y\bar{y}}=|x|\cdot|y|.$$

Для доказательства (8) сначала докажем равенство

$$|1+z|\leqslant 1+|z|. \tag{9}$$

Пусть $z=a+bi$. Тогда

$$|z|=\sqrt{a^2+b^2}\geqslant\sqrt{a^2}=|a|,$$

$$|1+z|^2=(1+z)(1+\bar{z})=1+(z+\bar{z})+z\bar{z}=1+2a+|z|^2\leqslant$$
$$\leqslant 1+2\cdot|z|+|z|^2=(1+|z|)^2,$$

откуда $|1+z|\leqslant 1+|z|$, т. е. (9) доказано.

Теперь докажем (8). Для $x=0$ неравенство (8), очевидно, выполнено. Если $x\neq 0$, то

$$|x+y|=|x\,(1+x^{-1}y)\,|=|x|\cdot|1+x^{-1}y|\leqslant|x|(1+|x^{-1}y|)=$$
$$=|x|+|x||x^{-1}y|=|x|+|xx^{-1}y|=|x|+|y|,$$

что и требовалось доказать.

Определения предела последовательности, фундаментальной последовательности и полноты поля (§ 24, определения 3—5) используют лишь понятия абсолютной величины элементов, а доказательства свойств этих понятий (§ 24, теоремы 1—3) используют лишь свойства абсолютной величины, доказанные в теореме 8 из § 9, т. е. $|a|>0$ для $a\neq 0$,

$$|ab|=|a||b|,\quad |a+b|\leqslant|a|+|b|.$$

Равенства (7) и (8) показывают, что модуль $|z|$ комплексного числа z обладает аналогичными свойствами. Поэтому в поле комплексных чисел имеют смысл понятие предела последовательности и другие вышеуказанные понятия и сохраняют силу многие из свойств этих понятий. Точно так же основные понятия и теоремы математического анализа сохраняют силу при переходе от поля действительных к полю комплексных чисел. Их рассмотрение составляет обширную и стройную теорию, называемую теорией функций комплексного переменного [1]).

---

[1]) См. Э. э. м., кн. 3, В. Л. Гончаров, Элементарные функции в комплексной области.

§ 30. Гиперкомплексные числа, кватернионы

В этом параграфе нам придётся пользоваться понятиями векторного пространства и основными его свойствами, а также свойствами многочленов с комплексными или действительными коэффициентами. Нужные свойства мы будем точно формулировать, но за их доказательствами отсылаем читателя ко второй книге «Энциклопедии» [1]).

Любое комплексное число представляется в виде

$$a+bi=a\cdot 1+bi$$

(§ 28, теорема 1), т. е. линейно выражается через два числа 1 и i с действительными коэффициентами a и b. После того как комплексные числа получили всеобщее признание в науке, естественно возник вопрос, нельзя ли построить числа, более общие, чем комплексные, которые линейно выражались бы через данные n из них с действительными коэффициентами. В середине XIX столетия английским математиком Гамильтоном были построены такие числа для $n=4$, названные им кватернионами. Однако для этого пришлось отказаться от коммутативности умножения. Позднее было доказано, что это не случайно: поле действительных чисел (при $n=1$) и поле комплексных чисел (при $n=2$) оказались единственными полями такого рода.

Имея в виду кватернионы и более общие системы, играющие в современной алгебре важную роль, мы в настоящем параграфе будем понимать под кольцом более общее образование, чем до сих пор. Именно, мы откажемся от коммутативности умножения (§ 7, свойства 1, IV). Тогда вместо одного закона дистрибутивности (§ 7, VI) надо требовать выполнения двух условий:

VI′. $$(a+b)c=ac+bc,\quad c(a+b)=ca+cb.$$

Соответствующее обобщение даётся понятию поля. Здесь вместо одного закона обратимости (§ 8, свойства I, VII) требуется:

VII′. *Для любых a и b, где $a\neq 0$, уравнения $ax=b$, $ya=b$ имеют решения.*

В отличие от колец здесь принято изменение терминологии. Множество P с операциями сложения и умножения, обладающими свойствами I — III, V из § 7, VI′ и VII′ и содержащее более одного элемента, называется *телом.*

Элементы тела, отличные от нуля, образуют группу (вообще говоря, некоммутативную). Поэтому, как и в случаях поля, тело обладает единицей, а всякий его элемент, отличный от нуля, — обратным элементом.

---

[1]) См. Э. э. м., кн. 2, А. И. Узков, Векторные пространства и линейные преобразования.

Определение 1. *Множество R называется n-мерным векторным пространством над данным полем P, если в R определена операция сложения, относительно которой R является коммутативной группой* (§ 6, определение 2), *и если, кроме того, определено умножение элементов из R на элементы поля P, обладающее следующими свойствами:*

1) *Произведение ax любого элемента a из P на любой элемент x из R есть некоторый элемент из R.*

2) $a(x+y)=ax+ay$ *для любых a из P и x, y из R.*

3) $(a+b)x=ax+bx$ *для любых a, b из P и x из R.*

4) $(ab)x=a(bx)$ *для любых a, b из P и x из R.*

5) *В R существует n элементов $e_1, \ldots, e_n$* (базис R) *таких, что любой элемент x из R однозначно представляется в виде*

$$x=a_1e_1+a_2e_2+\ldots+a_ne_n,$$

где $a_1, a_2, \ldots, a_n$ — элементы поля P, называемые компонентами вектора x.

Отсюда легко следует, что сложение двух векторов сводится к сложению их компонент и умножение вектора на элемент поля P — к умножению компонент на данный элемент. Поэтому n-мерное векторное пространство над полем P можно также определить, как совокупность всех упорядоченных систем $(a_1, a_2, \ldots, a_n)$ из n элементов поля P с указанными выше сложением и умножением на элементы из P.

Определение 2. *n-мерное векторное пространство R над полем P называется алгеброй* (или *гиперкомплексной системой*) *ранга n над полем P, если в R, кроме сложения, определена операция умножения, причём относительно этих двух операций R является кольцом* (не обязательно коммутативным) *и умножение в R связано с умножением его элементов на элементы из поля P следующим условием:*

6) $$(ax)y=x(ay)=a(xy)$$

для любых a из P и x, y из R.

Если при этом кольцо R является телом, то R называется алгеброй с делением.

Из 6) следует:

$$(ax)(by)=(ab)(xy) \tag{1}$$

для любых a, b из P и x, y из R.

Отсюда в силу законов дистрибутивности VI′ следует, что произведения любых элементов из R вполне определяются произведениями базисных элементов, так как если

$$x=\sum_{i=1}^{n}a_ie_i, \quad y=\sum_{j=1}^{n}b_je_j,$$

то

$$\left(\sum_{i=1}^{n} a_i e_i\right)\left(\sum_{j=1}^{n} b_j e_j\right) = \sum_{i,j=1}^{n} (a_i b_j)(e_i e_j). \tag{2}$$

Каждое произведение $e_i e_j$ в силу 5) линейно выражается через базис в виде

$$e_i e_j = \sum_{k=1}^{n} c_{ijk} e_k, \tag{3}$$

где c_{ijk} — элементы поля P, однозначно определяющие произведения $e_i e_j$.

Условиями (2) и (3) произведение любых элементов из R вполне определено, причём законы дистрибутивности VI′ будут автоматически выполнены. Для выполнения закона ассоциативности умножения для любых элементов из R достаточно потребовать его выполнение для элементов базиса. Это даёт условия

$$(e_i e_j) e_k = e_i (e_j e_k) \qquad (i, j, k = 1, 2, \ldots, n). \tag{4}$$

Вычисляя здесь произведение элементов базиса согласно (3), мы получаем условия, связывающие элементы c_{ijk}, при выполнении которых в R справедлив закон ассоциативности умножения. Таким образом, алгебры ранга n над полем P вполне определяются заданием поля P ранга n и n^3 элементов c_{ijk} $(i, j, k = 1, 2, \ldots, n)$ из поля P, удовлетворяющих условиям (3) и (4), где $e_1, e_2, \ldots, e_n$ — данный базис пространства R; n^3 элементов c_{ijk} поля P называются *структурными константами* или *постоянными умножения* данной алгебры R.

Приведём простейшие примеры алгебр.

Пример 1. Поле действительных чисел D является одномерным векторным пространством над тем же полем D с базисным элементом 1. Считая произведение ax вектора x на числа a совпадающим с обычным произведением чисел a и x, получим алгебру ранга 1 над полем D. При базисном элементе 1 единственная структурная константа $c_{111} = 1$. Если за базисный элемент принять любое число $a \neq 0$, то из $a^2 = a \cdot a$ следует, что новая структурная константа будет: $c'_{111} = a$. Очевидно, что D — алгебра с делением и притом коммутативная.

Пример 2. Поле комплексных чисел K является двумерным векторным пространством над полем действительных чисел D с базисом из двух элементов 1, i, так как любое комплексное число представляется в виде $a \cdot 1 + bi$ с действительными a и b. Считая произведение ax вектора x на действительное число a совпадающим с обычным произведением a и x, получим алгебру ранга 2 над D. Из правил умножения базисных элементов $(1 \cdot 1 = 1,$

$i \cdot i = -1$, $1 \cdot i = i \cdot 1 = i$) находим значения всех $2^3 = 8$ структурных констант в данном базисе:

$$c_{111} = 1, \quad c_{112} = 0, \quad c_{121} = 0, \quad c_{122} = 1,$$
$$c_{211} = 0, \quad c_{212} = 1, \quad c_{221} = -1, \quad c_{222} = 0;$$

K — коммутативная алгебра с делением.

Пример 3. Тело кватернионов. Существует ещё одна алгебра с делением над полем действительных чисел D и притом ранга 4. Это — алгебра кватернионов Q.

Будем считать, что Q содержит поле действительных чисел D. Приняв за первый элемент базиса число 1 и обозначив остальные его элементы через i, j, k, находим, что любой кватернион q единственным образом представляется в виде

$$q = a + bi + cj + dk, \tag{5}$$

где a, b, c, d — действительные числа. Для полного описания алгебры достаточно задать таблицу умножения базисных элементов. Мы положим:

$$\left.\begin{aligned} &i^2 = j^2 = k^2 = -1, \\ &ij = k, \quad jk = i, \quad ki = j, \\ &ji = -k, \; kj = -i, \quad ik = -j. \end{aligned}\right\} \tag{6}$$

Кроме того, число 1 обладает обычным свойством при умножении, т. е. $1 \cdot 1 = 1$, $1 \cdot i = i \cdot 1 = i$ и т. д.

Таким образом,

$$ij = -ji, \quad jk = -kj, \quad ki = -ik,$$

т. е. алгебра Q некоммутативна.

Остаётся проверить ассоциативность умножения базисных элементов (4). Так как соотношения (6) симметричны относительно i, j, k, то достаточно проверить равенства, в которых совпадают все три элемента, или два элемента, или все элементы различны, т. е. равенства

$$(ii)\,i = i\,(ii), \quad (ii)\,j = i\,(ij), \quad (ij)\,i = i\,(ji),$$
$$(ji)\,i = j\,(ii), \quad (ij)\,k = i\,(jk).$$

Проверку этих равенств предоставляем читателю.

Покажем, что алгебра Q является телом. Из того, что 1 обладает обычным свойством при умножении на элементы базиса, применяя свойства 2) и 6) и выражение (5) для кватернионов q, получим: $1 \cdot q = q \cdot 1 = q$ для любого q, т. е. число 1 играет роль единицы кольца Q.

Кватернион

$$\overline{q} = a - bi - cj - dk$$

называется *сопряжённым* кватерниону

$$q = a + bi + cj + dk.$$

Пользуясь таблицей умножения (6), законом дистрибутивности и соотношением (1), легко проверить, что

$$q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2.$$

Число

$$N(q) = a^2 + b^2 + c^2 + d^2$$

называется *нормой кватерниона* $q = a + bi + cj + dk$. Очевидно, что $N(q) = N(\bar{q})$ и $N(q) \geqslant 0$, причём $N(q) > 0$, если $q \neq 0$. Так как

$$q \cdot \frac{\bar{q}}{N(q)} = \frac{\bar{q}}{N(q)} \cdot q = 1$$

для любого $q \neq 0$, то любой кватернион $q \neq 0$ обладает обратным элементом

$$q^{-1} = \frac{\bar{q}}{N(q)}.$$

Отсюда уже следует (см. § 6), что множество всех кватернионов, отличных от нуля, образует группу относительно операции умножения. Поэтому кольцо Q является телом, т. е. алгеброй с делением над полем действительных чисел D.

Для ознакомления с другими свойствами кватернионов, в частности с их геометрическим представлением, отсылаем читателя к книге Э. Чезаро [14], стр. 393—412.

Мы рассмотрели три алгебры с делением над полем действительных чисел, а именно ранга 1, 2 и 4. Справедлива замечательная теорема о том, что других алгебр такого типа не существует. Точнее любая алгебра с делением над полем действительных чисел изоморфна одной из этих трёх алгебр.

Чтобы доказать это, сделаем несколько замечаний, касающихся алгебры над любым полем P. Если читателя затрудняет рассмотрение любого поля, то он может ограничиться нужным для дальнейшего случаем поля действительных чисел.

Замечание 1. *Любой элемент x алгебры R над полем P является корнем некоторого многочлена с коэффициентами из поля P, не все из которых равны нулю.*

В самом деле, если n — ранг R, то любые $n+1$ элементов $x_1, \ldots, x_{n+1}$ из R линейно зависимы. В частности, элементы $x, x^2, \ldots, x^{n+1}$ линейно зависимы, т. е. $a_1 x + a_2 x^2 + \ldots + a_{n+1} x^{n+1} = 0$, где $a_1, a_2, \ldots, a_{n+1}$ не все равны нулю. Это значит, что элемент x является корнем многочлена $a_1 z + a_2 z^2 + \ldots + a_{n+1} z^{n+1}$ с коэффициентами из P.

Замечание 2. Равенства вида $f(z)+g(z)=h(z)$ и $f(z)\cdot g(z)=h(z)$, где $f(z)$, $g(z)$, $h(z)$ — многочлены от одного неизвестного z с коэффициентами из поля P[1]), сохраняют силу при замене неизвестного z любым элементом x алгебры R над полем P.

В самом деле, из 3) следует, что $f(x)+g(x)=h(x)$ Далее, $x^m\cdot x^n=x^{m+n}$ [§ 6, (3)]. Отсюда из законов дистрибутивности VI и из соотношений (1) и 3) следует, что

$$f(x)\cdot g(x)=h(x).$$

Замечание 3. Если алгебра R над полем P содержит единицу e (в частности, если R — алгебра с делением), то R изоморфна алгебре, содержащей поле P. В самом деле, из 3) и (1) следует:

$$a_1e+a_2e=(a_1+a_2)\,e,$$

$$(a_1e)\,(a_2e)=(a_1a_2)\,(ee)=(a_1a_2)\,e.$$

Таким образом, множество P' всех элементов алгебры R вида ae изоморфно полю P (§ 9, определение 2). По теореме 2 из § 9 (где коммутативность умножения несущественна) существует кольцо R', содержащее P и изоморфное кольцу R. Определим произведение ax' элемента a из P на элемент x' из R' как элемент R', соответствующий произведению ax из R, где x — элемент из R, соответствующий элементу x' Нетрудно показать, что тогда R' будет алгеброй над полем P, причём для элемента x' из P определённое выше произведение ax' совпадает с произведением элементов a и x', заданным в поле P. Поэтому единица поля P будет в то же время единицей алгебры R'.

Замечание 4. Алгебра с делением не имеет делителей нуля (§ 7, определение 2). Доказывается это так же, как в случае полей: если $xy=0$ и $x\neq 0$, то, умножая обе части равенства слева на x^{-1}, получим: $y=0$.

Теорема 1. *Любая коммутативная алгебра с делением R над полем действительных чисел D изоморфна либо полю действительных чисел D, либо полю комплексных чисел R и имеет ранг* 1 *или* 2. *Обратно, любая алгебра с делением R над полем действительных чисел D ранга* 1 *или* 2 *изоморфна соответственно полю действительных или комплексных чисел и коммутативна.*

Доказательство. а) Пусть R — алгебра с делением над полем действительных чисел D, содержащая D, но не совпадающая с D.

Покажем, что для любого элемента x, не входящего в D, существуют действительные числа a и b, где $a\neq 0$, такие, что эле-

---

[1]) Понятие многочлена и операций сложения и умножения с коэффициентами из некоторого поля P вполне аналогично соответствующим понятиям для многочленов с числовыми коэффициентами. Разница лишь в том, что коэффициенты многочленов будут не числами, а элементами данного поля P.

мент $i=ax+b$ обладает свойством $i^2=-1$. (Заметим для дальнейшего, что при этом мы не пользуемся коммутативностью алгебры R.) Согласно замечанию 1 элемент x является корнем многочлена $f(z)$ с действительными коэффициентами, не все из которых равны нулю. Но известно, что любой такой многочлен разлагается на множители первой или второй степени с действительными коэффициентами [1]). Пусть

$$f(z)=f_1(z)f_2(z)\dots f_k(z)$$

такое разложение. Тогда, согласно замечанию 2,

$$f(x)=f_1(x)f_2(x)\dots f_k(x).$$

Но $f(x)=0$, и по замечанию 4 алгебра R не имеет делителей нуля. Поэтому $f_l(x)=0$ для некоторого $l\leqslant k$. Если x — корень многочлена $z-c$ первой степени, то $x-c=0$, $x=c$, т. е. x принадлежит полю D, что противоречит условию. Таким образом, x есть корень многочлена второй степени, т. е. $x^2+px+q=0$, где p и q — действительные числа, причём $\frac{p^2}{4}-q<0$, ибо иначе x был бы корнем многочлена первой степени. Полагая

$$\frac{p^2}{4}-q=-t^2$$

с действительным t, получим:

$$\left(x+\frac{p}{2}\right)^2=\frac{p^2}{4}-q=-t^2,$$

откуда, деля на t^2, находим:

$$\left(\frac{x+\frac{p}{2}}{t}\right)^2=-1.$$

Полагая $a=\frac{1}{t}$ и $b=\frac{p}{2t}$, получим элемент $i=ax+b$, для которого $i^2=-1$, что и нужно.

б) Пусть R — коммутативная алгебра с делением над полем действительных чисел D, содержащая D. Если $R\neq D$, то по доказанному в R существует элемент i такой, что $i^2=-1$. Поэтому элемент i не входит в D и элементы 1, i линейно независимы. Пусть R_0 — множество всех элементов x алгебры R вида $x=a+bi$ с любыми действительными a и b. Очевидно, что R_0 — алгебра ранга 2 над полем D — изоморфна полю комплексных чисел R.

Покажем, что $R_0=R$. Полагая, $b=0$ в равенстве $x=a+bi$, получим: $x=a$. Следовательно, R_0 содержит поле действительных

[1]) См. Э. э. м., кн. 2, Л. Я. Окунев, Кольцо многочленов и поле рациональных функций, гл. I, § 6.

чисел D. Пусть x — любой элемент алгебры R, не входящий в D. По доказанному в пункте а) существуют действительные числа c, d, где $c \neq 0$, для которых элемент $j = cx + d$ обладает свойством $j^2 = -1$. Из коммутативности R следует, что $ij = ji$, откуда

$$(i+j)(i-j) = i^2 - ij + ji - j^2 = 0.$$

Так как согласно замечанию 4 в R отсутствуют делители нуля, то либо $i - j = 0$, либо $i + j = 0$, т. е. $j = \pm i$, а потому

$$x = -\frac{d}{c} + \frac{1}{c} j = -\frac{d}{c} \pm \frac{1}{c} i.$$

Поэтому x принадлежит R_0, откуда $R_0 = R$.

Итак, алгебра R либо совпадает с D, либо изоморфна полю комплексных чисел R. Согласно замечанию 3 любая коммутативная алгебра с делением над полем действительных чисел изоморфна некоторой алгебре R (очевидно, также коммутативной и с делением), т. е. изоморфна либо полю действительных чисел D, либо полю комплексных чисел R.

в) Пусть R — любая алгебра с делением ранга 1 над полем действительных чисел D, содержащим D. Приняв за базисный элемент число 1, получим, что любой элемент x из R имеет вид $x = a \cdot 1 = a$ с действительным a, следовательно, $R = D$. По замечанию 3 любая алгебра с делением ранга 1 над D изоморфна полю действительных чисел D.

г) Пусть R — любая алгебра с делением ранга 2 над полем действительных чисел D, содержащая D. Тогда $R \neq D$. По доказанному в пункте а) в R существует элемент i со свойством $i^2 = -1$. Элементы 1, i линейно независимы, так как иначе $a_1 \cdot 1 + a_2 i = 0$ с действительными a_1, a_2, отличными от нуля (ибо в силу отсутствия делителей нуля из $a_1 = 0$ следует $a_2 = 0$, и обратно). Тогда $i = -\frac{a_1}{a_2}$, т. е. принадлежит D, что невозможно ввиду $i^2 = -1$ (§ 10, теорема 7). Так как в n-мерном векторном пространстве любые n линейно независимых векторов образуют базис [1]) и R — алгебра ранга 2, то элементы 1, i образуют базис. Таким образом, любой элемент x из R однозначно представляется в виде $x = a + bi$ с действительными a и b. Если $x = a + bi$ и $y = c + di$ — любые два элемента из R, то из таблицы умножения элементов легко находим:

$$x + y = (a + c) + (b + d) i,$$
$$xy = (ac - bd) + (ad + bc) i.$$

Итак, алгебра R изоморфна полю комплексных чисел K. По замечанию 3 любая алгебра с делением ранга 2 над полем

---

[1]) См. Э. э. м., кн. 2, А. И. Узков, Векторные пространства и линейные преобразования.

действительных чисел D изоморфна полю комплексных чисел K. Теорема доказана.

Если отказаться от коммутативности умножения, то возможна ещё одна алгебра с делением над полем D — алгебра кватернионов, а именно:

Теорема 2. (Теорема Фробениуса.) *Любая алгебра с делением R над полем действительных чисел D изоморфна полю действительных чисел D, либо полю комплексных чисел K, либо телу кватернионов Q и имеет ранг* 1, 2 *или* 4.

Доказательство. Пусть R — любая алгебра с делением ранга n над полем действительных чисел D, содержащая D. По теореме 1, если $n=1$, то R изоморфна полю действительных чисел D, а если $n=2$, — полю комплексных чисел K. Пусть R имеет ранг $n>2$. Тогда $R\neq D$. По доказанному в пункте а) в R существует элемент i, для которого $i^2=-1$.

Как в пункте г), докажем, что элементы 1, i линейно независимы. Так как ранг R больше двух, то в R существует элемент x, который нельзя представить в виде $a+bi$ с действительными a и b. По доказанному в пункте а) существуют действительные числа a' и b', где $a'\neq 0$, такие, что элемент $x_1=a'x+b'$ обладает свойством $x_1^2=-1$. Элемент x_1 нельзя представить в виде $a+bi$ с действительными a и b, так как иначе и элемент

$$x=\frac{1}{a'}x_1-\frac{b'}{a'}$$

также представлялся бы в указанном виде. Поэтому элементы 1, i, x_1 линейно независимы. В самом деле, если

$$a_1\cdot 1+a_2i+a_3x_1=0$$

с действительными a_1, a_2, a_3, то $a_3=0$ (ибо иначе x_1 линейно выражался бы через 1, i), а по линейной независимости 1, i тогда также $a_1=a_2=0$. Рассуждая, как в пункте а), находим, что элементы $i+x_1$ и $i-x_1$ являются корнями квадратных уравнений с действительными коэффициентами, откуда

$$(i+x_1)^2=p(i+x_1)+q,$$
$$(i-x_1)^2=r(i-x_1)+s.$$

Поэтому

$$\left.\begin{aligned}-2+ix_1+x_1i&=p(i+x_1)+q,\\ -2-ix_1-x_1i&=r(i-x_1)+s,\end{aligned}\right\}\qquad(7)$$

где p, q, r, s — действительные числа.

Складывая эти равенства, получаем:

$$-4=(p+r)i+(p-r)x_1+(q+s),$$

откуда в силу линейной независимости элементов 1, i, x_1 находим:

$$p+r=0, \quad p-r=0, \quad \text{т. е} \quad p=r=0.$$

Тогда из (7) следует:

$$ix_1+x_1i=2t, \tag{8}$$

где $t=\frac{1}{2}(q+2)$ — действительное число. Положим теперь $x_2=$ $=x_1+ti$; элементы 1, i, x_2 линейно независимы, так как иначе элементы 1, i, x_1 были бы линейно зависимы. Из (8) следует:

$$x_2^2=-1+t(ix_1+x_1i)-t^2=t^2-1.$$

Число t^2-1 — отрицательное действительное число, так как если $t^2-1>0$, то $t^2-1=u^2$ с действительным u. Из перестановочности x_2 и u находим:

$$(x_2+u)(x_2-u)=x_2^2-u^2=0,$$

т. е. $x_2=\pm u$ — действительное число, что противоречит линейной независимости элементов 1, i, x_2.

Положим $x_2^2=-c^2$, где c — действительное число и пусть $j=\frac{1}{c}x_2$.

Тогда $j^2=-1$ и элементы 1, i, j линейно независимы, ибо 1, i, x_2 линейно независимы.

Далее, в силу (8)

$$ij+ji=i\cdot\frac{1}{c}(x_1+ti)+\frac{1}{c}(x_1+ti)\,i=$$

$$=\frac{1}{c}(ix_1+ti^2+x_1i+ti^2)=\frac{1}{2}(2t-t-t)=0,$$

откуда

$$ij=-ji. \tag{9}$$

Положим $k=ij$ и покажем, что k нельзя выразить линейно через 1, i, j. Если $k=a+bi+cj$ с действительными a, b, c, то, умножая это равенство слева на i, получим:

$$ik=i(ij)=-j=ai-b+ck=ai-b+c(a+bi+cj),$$

откуда

$$(ac-b)+(a+bc)i+(c^2+1)j=0,$$

и в силу линейной независимости элементов 1, i, j должно быть $c^2+1=0$, $c^2=-1$, что невозможно, так как c — число действительное. Рассуждая, как выше (для 1, i, x_1) докажем, что элементы 1, i, j, k линейно независимы. Таким образом, ранг алгебры R не меньше четырёх.

Покажем, что элементы i, j, k обладают таблицей умножения (6). Мы уже имеем: $i^2=j^2=-1$ и $j=k$. Далее, в силу (9):

$$k^2=(ij)(ij)=i(ji)j=i(-ij)j=-1,$$
$$jk=j(ij)=j(-ji)=i, \quad ki=(ij)i=(-ji)i=j,$$
$$ji=-ij=-k, \quad kj=(ij)j=-i, \quad ik=i(ij)=-j.$$

Таким образом, все соотношения (6) выполнены. Как было отмечено в конце замечания 3, число 1 является единицей алгебры R. Поэтому совокупность Q всех элементов x из R, имеющих вид $x=a+bi+cj+dk$, с действительными a, b, c, d является телом кватернионов. Покажем, что $R=Q$. В противном случае в R существует элемент y, не принадлежащий Q. По доказанному в пункте а) существуют действительные числа a и b, где $a\neq 0$, такие, что элемент $l=ay+b$ обладает свойством $l^2=-1$, элемент l лежит вне Q, так как иначе $y=\frac{1}{a}l-\frac{b}{a}$ лежал бы в Q. Рассуждая, как при выводе (8), найдём:

$$il+li=a, \quad jl+lj=b, \quad kl+lk=c,$$

где a, b, c — действительные числа. Отсюда находим:

$$lk=l(ij)=(li)j=(a-il)j=aj-i(lj)=$$
$$=aj-i(b-jl)=aj-bi+kl=aj-bi+c-lk,$$

т. е.

$$2lk=c-bi+aj.$$

Умножая это равенство справа на k, получим:

$$-2l=ai+bj+ck,$$

т. е. элемент l принадлежит Q, что невозможно, следовательно, $R=Q$. Итак, либо $R=D$, либо $R=K$, либо $R=Q$. Согласно замечанию 3 любая алгебра с делением над полем действительных чисел D изоморфна алгебре R (также с делением), содержащей D, т. е. изоморфна либо полю действительных чисел D, либо полю комплексных чисел K, либо телу кватернионов. Теорема доказана.

Заменяя в примерах 1—3 поле действительных чисел D полем рациональных чисел Γ получим ещё три алгебры с делением, но уже над полем Γ, именно: само поле рациональных чисел Γ, поле комплексных чисел вида $a+bi$ с рациональными a и b (так называемое *числовое поле Гаусса*) и тело рациональных кватернионов, т. е. кватернионов вида $a+bi+cj+dk$ с рациональными a, b, c и d.

Заметим, что, заменяя в тех же примерах 1—3 поле действительных чисел D на поле комплексных чисел K, мы в примере 1

получим само поле K, а в примерах 2 и 3 получим алгебры над K, уже не являющиеся алгебрами с делением. В самом деле, согласно замечанию 1 любой элемент x алгебры R над K, содержащей K, является корнем многочлена $f(z)$ с комплексными коэффициентами. Известно [1]), что любой многочлен с комплексными коэффициентами разлагается на множители первой степени также с комплексными коэффициентами. Если R — алгебра с делением, то, рассуждая, как в а), найдём, что x является корнем многочлена первой степени с комплексными коэффициентами и, следовательно, сам является комплексным числом. Поэтому $R=K$.

Итак, если R есть алгебра над полем K ранга, большего единицы (как в примерах 2 и 3), то она не является алгеброй с делением.

Литература

1. Александров П. С., Введение в общую теорию множеств и функций, Гостехиздат, М.—Л., 1948.
2. Лузин Н. Н., Теория функций действительного переменного, Учпедгиз, М., 1948.
3. Окунев Л. Я., Основы современной алгебры, Учпедгиз, 1941.
4. Ван дер Варден Б. Л., Современная алгебра, ч. I, Гостехиздат, 1947.
5. Проскуряков И. В., Числа и многочлены, Издательство АПН РСФСР, 1949.
6. Шмидт О. Ю., Абстрактная теория групп, Гостехиздат, 1933.
7. Курош А. Г., Теория групп, Гостехиздат, 1944.
8. Ефимов Н. В., Высшая геометрия, 2-е изд., Гостехиздат, 1949.
9. Костин В. И., Основания геометрии, 2-е изд., Учпедгиз, М.—Л., 1948.
10. Дедекинд Э., Непрерывность и иррациональные числа, Одесса, 1923.
11. Хинчин А. Я., Восемь лекций по математическому анализу, Гостехиздат, 1943.
12. Курош А. Г., Курс высшей алгебры, 2-е изд., Гостехиздат, М.—Л., 1950.
13. Кузьмин Р. О. и Фаддеев Д. К., Алгебра и арифметика комплексных чисел, Учпедгиз, 1939.
14. Чезаро Э., Элементарный учебник алгебраического анализа и исчисления бесконечно малых, ОНТИ, 1936.

---

[1]) См. Э. э. м., кн. 2, Л. Я. Окунев, Кольцо многочленов и поле рациональных функций, гл. I, § 6.

А. Я. ХИНЧИН

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

*

ГЛАВА I

ДЕЛИМОСТЬ И ПРОСТЫЕ ЧИСЛА

§ 1. Введение

Значительная часть наиболее актуальных проблем теории целых чисел от глубокой древности до наших дней прямо или косвенно связана с понятием *делимости* чисел. Причину этого явления легко понять: из четырёх основных арифметических действий только деление не всегда выполнимо в области целых чисел, и поэтому только в отношении деления можно разумным образом ставить вопрос о том, *при каких условиях* оно выполнимо. Уже самые элементарные понятия теории делимости — наибольший общий делитель, наименьшее общее кратное, взаимно простые числа, абсолютно простые числа и т. п. — не имеют себе никаких аналогов в случае других арифметических действий именно в силу неограниченной выполнимости этих действий.

С другой стороны, исторический ход развития арифметической науки показал, что теория делимости чисел, исходя из простейших и наиболее естественных задач, связанных с этим понятием, неизбежно и очень скоро приходит к образованию новых, более сложных понятий и к постановке новых, более трудных задач. Общеизвестно, как часто здесь возникают задачи, не только содержание, но и естественность постановки которых понятны и убедительны даже учащемуся средней школы, между тем как решение их подчас веками не поддаётся усилиям величайших учёных. Это делает понятным, почему учение о целых числах всегда казалось учёным неисчерпаемым полем для исследования и во все времена привлекало к себе внимание наиболее выдающихся умов.

В этих исследованиях русские, а позднее советские научные школы всегда занимали и до сих пор занимают одно из ведущих мест. Со времён Эйлера наша Академия наук давала — и даёт до настоящего времени — блестящие образцы создания как новых глубоких проблем, так и сильнейших методов их решения. Достаточно упомянуть созданную нашим великим Чебышевым замечательную школу арифметических исследований, равной которой за

последнее столетие не было и нет во всём мире и традиции которой в руках блестящей плеяды советских математиков и сегодня ещё приводят к глубочайшим достижениям [1]).

Нам предстоит здесь в кратком очерке проследить развитие некоторых разделов этого учения от древнейших времён до наших дней, уделяя — там, где это нужно, — особое внимание методологической и педагогической стороне дела.

§ 2. Однозначное разложение чисел на простые множители

Для всех многообразных разветвлений теории делимости центральное место занимает теорема об однозначной разложимости чисел на простые множители:

Основная теорема. *Всякое натуральное число, кроме* 1, *может быть представлено как произведение простых множителей; это представление единственно, если отвлечься от порядка множителей.*

Последнее означает, что если мы имеем

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

где все p_i и q_j — простые числа, то $s = r$ и числа q_j лишь порядком расположения могут отличаться от чисел p_i.

Примечание. Число $p > 1$ называется *простым* (или абсолютно простым), если оно не имеет других делителей, кроме p и 1. Все другие числа, превосходящие 1, называются *составными*; число 1 занимает особое положение, не будучи ни простым, ни составным. К сожалению, до недавнего времени почти все наши учебники причисляли единицу к простым числам; да и сейчас ещё сохранились среди методистов влиятельные сторонники этой традиции, несмотря на её грубую ошибочность, многократно доказанную. Вопрос о том, считать ли единицу простым числом, не есть, как это могло бы казаться, вопрос терминологии или вкуса. Называя единицу простым числом, мы немедленно делаем неверными почти все теоремы, связанные с простыми числами. Достаточно указать, что только что формулированная нами основная теорема при этом становится неверной, ибо, например, число 5 может быть разложено на простые множители бесконечным множеством способов:

$$5 = 1 \cdot 5 = 1 \cdot 1 \cdot 5 = 1 \cdot 1 \cdot 1 \cdot 5 = \ldots;$$

если 1 — простое число, то все эти разложения различны между собою (хотя бы потому, что число множителей в них различно).

---

[1]) Важнейшие этапы развития этой школы очень детально изложены в книге Б. Н. Делоне, Петербургская школа теории чисел, Издательство АН СССР, 1947.

Перейдём теперь к доказательству основной теоремы, которое во многих отношениях представляет методологический интерес.

Прежде всего очень легко доказать возможность разложения. Пусть $n > 1$ — любое натуральное число. Среди его делителей существуют числа, превосходящие 1 (например, само число n). Пусть p_1 — наименьший из таких его делителей; очевидно, p_1 есть простое число, ибо иначе оно имело бы такой делитель a, что $1 < a < p_1$; но a, будучи делителем p_1, было бы и делителем числа n, что, очевидно, противоречит определению числа p_1; итак, $n = p_1 n_1$, где p_1 — простое число. Если $n_1 > 1$, то, поступая с ним так же, как мы только что поступили с числом n, мы представим его в виде $n_1 = p_2 n_2$, где p_2 — простое число; отсюда $n = p_1 p_2 n_2$; если ещё $n_2 > 1$, то этот процесс, очевидно, можно продолжать и далее. Так как при этом $n > n_1 > n_2 > \dots$, то проводимый нами процесс после конечного числа шагов должен прекратиться, что может наступить лишь при условии, что какое-либо $n_k = 1$. Но тогда

$$n = p_1 p_2 \dots p_k,$$

где $p_1, p_2, \dots, p_k$ — простые числа. Этим и доказана возможность разложения любого натурального числа $n > 1$ на простые множители.

Теперь мы должны убедиться в единственности такого разложения, что представляет собою задачу значительно более трудную. Исторически очень интересно, что неочевидность этой единственности (а значит, и необходимость её доказательства) была осознана сравнительно поздно, после того как долгое время уже пользовались ею как самоочевидным фактом. Повидимому, Гаусс впервые настойчиво указывал на то, что невозможность двух существенно различных разложений одного и того же числа на простые множители отнюдь не самоочевидна и нуждается в строгом доказательстве. Даже такие выдающиеся учёные, как, например, Лежандр, писавший незадолго до Гаусса, не замечали этого. Дальнейшее развитие теории чисел показало, в какой мере Гаусс оказался прав не только с формально-логической, но и с идейной точки зрения. В XIX столетии учёным пришлось исследовать законы делимости для областей, более сложных, чем числа натурального ряда, — для так называемых целых алгебраических чисел. Законы эти во многом напоминали то, что мы имеем в области натуральных чисел, но вместе с тем иногда оказывались и существенно иными; в частности, здесь имеются простые числа, и любое число разлагается на простые множители; но *разложение это, вообще говоря, неоднозначно,* и именно это обстоятельство создало в арифметике алгебраических чисел новую, своеобразную трудность, совершенно незнакомую обычной арифметике натуральных чисел и в настоящее время успешно преодолённую.

Доказательство единственности разложения натуральных чисел на простые множители обычно имеет своим основанием следующее весьма замечательное предложение, которое оказывается полезным и во многих других задачах теории чисел.

Теорема 1. *Если натуральные числа a и b взаимно просты, то существуют такие целые числа x и y, что*

$$ax - by = 1.$$

Эту теорему обычно доказывают, опираясь на алгорифм Евклида и теорию цепных дробей. Мы увидим в главе III, как это может быть сделано. Здесь же мы приведём другое, методологически очень поучительное доказательство, данное Гауссом и свободное от применения каких бы то ни было алгорифмов.

Пусть d есть наименьшее положительное число, которое может быть представлено в виде

$$d = ax - by \tag{1}$$

при надлежащем выборе целых чисел x и y. Мы должны доказать, что $d = 1$; а так как числа a и b взаимно просты, т. е. не имеют других положительных общих делителей, кроме 1, то для этого достаточно убедиться, что как a, так и b делятся на d. В силу полного равноправия чисел a и b достаточно, разумеется, провести доказательство для какого-нибудь одного из них; мы покажем, что a делится на d.

Пусть a при делении на d даёт в частном m и в остатке r, так что

$$a = md + r \qquad (0 \leqslant r < d).$$

Отсюда

$$r = a - md = a - m(ax - by) = a(1 - mx) - b(-my) = ax' - by',$$

где положено:

$$x' = 1 - mx, \quad y' = -my.$$

Таким образом, число r может быть представлено в виде $ax' - by'$ с целыми x', y'. Так как $r < d$, а d есть по определению наименьшее положительное число, представимое в форме $ax - by$, то число r не может быть положительным; следовательно, $r = 0$ и $a = md$, т. е. a делится на d, что и требовалось доказать.

Заметим, что мы в сущности доказали теорему, применимую к любым целым числам a и b (не обязательно взаимно простым), а именно:

Наименьшее положительное число d, представимое в виде $ax - by$ с целыми x и y, есть наибольший общий делитель чисел a и b.

В самом деле, что d есть общий делитель чисел a и b, нами уже доказано; но этот общий делитель является наибольшим, так

как само соотношение (1) показывает, что d делится на любое число, служащее общим делителем чисел a и b.

Заметим, наконец, что весь этот круг вопросов, в особенности если присоединить к нему то, что будет по этому поводу изложено в главе III, в связи с алгорифмом Евклида, может служить превосходным — нетрудным и вместе с тем увлекательным — материалом для работы математического кружка средней школы.

Воспользуемся теперь теоремой 1 для доказательства следующего очень важного предложения теории делимости (известного уже Евклиду):

Теорема 2. *Если числа a и b взаимно просты, а произведение ac делится на b, то и число c делится на b.*

В самом деле, в силу теоремы 1 целые числа x и y могут быть выбраны так, что

$$ax - by = 1,$$

откуда

$$acx - bcy = c.$$

Так как по условию ac делится на b, то пусть $ac = bk$, где k — целое число; мы получаем:

$$c = acx - bcy = bkx - bcy = b(kx - cy),$$

откуда и видно, что c делится на b.

Пусть теперь p — простое число и a — любое натуральное число; очевидно, что тогда возможно только одно из двух: либо a делится на p, либо a взаимно просто с p. В самом деле, если a не взаимно просто с p, то a и p имеют общего делителя $d > 1$; но p, будучи числом простым, делится только на 1 и p; поэтому $d = p$ и a делится на p.

Это простое замечание позволяет вывести из теоремы 2 следующее важное

Следствие. *Если произведение ab делится на простое число p, то по меньшей мере один из сомножителей делится на p.*

В самом деле, если, например, a не делится на p, то в силу только что сделанного замечания a взаимно просто с p; но тогда из делимости произведения ab на p в силу теоремы 2 вытекает, что b делится на p, что и требовалось доказать.

Это правило, доказанное нами для произведения двух сомножителей, легко способом индукции распространить и на любое число сомножителей. Пусть, например, произведение abc делится на простое число p; если a не делится на p, то согласно доказанному произведение bc должно делиться на p, а тогда, как мы знаем, либо b, либо c делится на p. В конечном счёте, следовательно, из делимости на простое число p произведения abc вытекает делимость на p по меньшей мере одного из сомножителей. Таким же путём от трёх сомножителей можно, очевидно, перейти к четырём,

пяти и вообще любому числу сомножителей. Таким образом, мы можем считать установленным следующее общее предложение, которое и было целью всех предшествующих рассуждений:

Теорема 3. *Если произведение нескольких чисел делится на простое число p, то по меньшей мере один из сомножителей делится на p.*

Теорема 3 позволяет уже легко установить единственность разложения любого натурального числа (кроме 1) на простые множители. В самом деле, пусть мы имеем:

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \tag{2}$$

где все p_i и все q_j — простые числа; требуется доказать, что числа $q_1, q_2, \dots, q_s$ лишь порядком расположения могут отличаться от чисел $p_1, p_2, \dots, p_r$. Другими словами, если предположить, что как числа p_i, так и числа q_j расположены в порядке возрастания (т. е. $p_1 \leqslant p_2 \leqslant \dots \leqslant p_r$, $q_1 \leqslant q_2 \leqslant \dots \leqslant q_s$), то требуется просто доказать, что $r = s$ и $p_i = q_i (1 \leqslant i \leqslant r)$. Именно так мы и поступим.

Докажем сначала, что $p_1 = q_1$. В самом деле, пусть, например, $q_1 > p_1$. В силу равенства (2) произведение $q_1 q_2 \dots q_s$ делится на p_1; поэтому в силу теоремы 3 по меньшей мере одно из чисел q_j делится на p_1; но все q_j — простые числа, а потому то из них, которое делится на p_1, должно просто совпадать с p_1; это же невозможно, так как согласно нашему предположению

$$p_1 < q_1 \leqslant q_2 \leqslant \dots \leqslant q_s.$$

Итак, $p_1 = q_1$; но тогда соотношение (2) даёт:

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Очевидно, отсюда мы можем, в точности повторяя только что проведённое рассуждение, доказать, что $p_2 = q_2$; это же даёт:

$$p_3 p_4 \dots p_r = q_3 q_4 \dots q_s,$$

откуда $p_3 = q_3$ и т. д. Этот процесс мы можем продолжать до тех пор, покуда и налево, и направо у нас ещё сохраняются простые множители; он обрывается, как только тут или там простые множители исчерпаны; но очевидно, что это должно наступить налево и направо одновременно, т. е. что мы должны иметь $r = s$. В самом деле, если бы, например, мы имели $r < s$, то согласно вышесказанному доказали бы, что $p_1 = q_1$, $p_2 = q_2$, $\dots$, $p_r = q_r$, и после сокращений получили бы:

$$1 = q_{r+1} q_{r+2} \dots q_s,$$

что очевидным образом неверно. Итак,

$$r = s,$$

и

$$p_1 = q_1, \quad p_2 = q_2, \quad \dots, \quad p_r = q_r,$$

т. е. оба разложения числа n на простые множители полностью совпадают между собою. Этим фундаментальная теорема теории делимости полностью доказана.

Мы видим, что ключом к её доказательству нам служила важная теорема 2. Все доказательства фундаментальной теоремы так или иначе базируются на этом предложении; различия их касаются лишь того пути, каким мы приходим к теореме 2. Выше мы выбрали путь, идущий через теорему 1. Методологически этот путь важен и интересен тем, что он не предполагает известными свойства наибольшего общего делителя и наименьшего общего кратного двух чисел (для реализации этого пути нет даже надобности в знакомстве с этими двумя понятиями); дело в том, что исследование этих двух понятий с максимальной простотой и прозрачностью проводится, как известно, на основе самой фундаментальной теоремы.

Однако методологически интересно показать, что решающая теорема 2 может быть доказана и совсем иным путём, обходящимся без теоремы 1 и опирающимся на элементарные свойства наименьшего общего кратного двух чисел. Проследим теперь этот путь.

Прежде всего здесь надо установить структуру совокупности всех общих кратных двух данных чисел a и b, т. е. всех чисел, делящихся как на a, так и на b. Если m — наименьшее положительное число, делящееся на a и на b (т. е. наименьшее общее кратное чисел a и b), а m' — какое-либо другое общее кратное тех же чисел, то пусть q — частное, а r — остаток от деления m' на m, так что

$$m' = qm + r \qquad (0 \leqslant r < m);$$

отсюда

$$r = m' - qm.$$

Так как m' и m оба делятся на a и b, то число r также будет общим кратным чисел a и b; но $r < m$, а m есть наименьшее положительное общее кратное чисел a и b. Следовательно, $r = 0$ и $m' = qm$, т. е. *всякое общее кратное чисел a и b делится на m*. Так как, очевидно, и обратно — всякое число вида qm есть общее кратное чисел a и b, то *совокупность общих кратных чисел a и b совпадает с совокупностью чисел, кратных некоторого одного числа m* (которое есть наименьшее общее кратное чисел a и b).

Теперь мы покажем, что *наименьшее общее кратное двух взаимно простых чисел равно их произведению.*

Пусть числа a и b взаимно просты и m — их наименьшее общее кратное. Так как произведение ab есть общее кратное чисел a и b, то согласно предыдущему

$$ab = qm,$$

где q — целое число. Но вытекающие отсюда соотношения

$$\frac{a}{q}=\frac{m}{b}, \quad \frac{b}{q}=\frac{m}{a}$$

показывают, что q есть общий делитель взаимно простых чисел a и b; следовательно, $q=1$ и $m=ab$, что и требовалось доказать.

Теперь уже совсем легко установить теорему 2. Так как, по предположению, ac есть общее кратное взаимно простых чисел a и b, то ac делится на наименьшее общее кратное этих чисел, которое, как мы только что установили, равно ab. Делимость же ac на ab равносильна делимости c на b, чем теорема 2 и доказана.

§ 3. О простых числах

Простые числа в теории делимости играют роль первичных, неразложимых элементов, из которых путём перемножения затем создаются все другие натуральные числа, как этому учит вышеустановленная фундаментальная теорема. Множество простых чисел служит как бы мультипликативным (т. е. развивающимся путём перемножения) базисом натурального ряда. Эта основоположная роль совокупности простых чисел во все времена привлекала к ней внимание исследователей. Каково это множество, сколько чисел оно содержит, как эти числа расположены, каким закономерностям подчиняется чередование простых и составных чисел в натуральном ряду? Все эти вопросы естественно вставали перед учёными самых различных эпох, от античного мира до наших дней, и в значительной степени они стоят ещё в центре внимания и современной арифметической науки, в особенности потому, что решение их оказалось связанным с чрезвычайно большими трудностями.

Прежде всего здесь, разумеется, встаёт вопрос о том, конечно или бесконечно множество простых чисел. Важно отметить, что фундаментальная теорема, доказанная нами выше, ничего об этом не говорит, по крайней мере непосредственно. Её утверждение как будто бы ничем не противоречит ни конечности, ни бесконечности множества простых чисел.

Эта задача была единственной проблемой теории простых чисел, которую удалось решить математикам древнего мира. Приведём простое и остроумное рассуждение Евклида, доказывающее бесконечность множества простых чисел; впрочем, идея бесконечности, столь излюбленная современной наукой, была чужда Евклиду, и он формулирует свою теорему так: *простых чисел имеется больше, чем любое число их.* («Начала Евклида», кн. IX, предложение 20.)

Пусть $p_1, p_2, \ldots, p_k$ — любая конечная группа простых чисел. Требуется доказать, что найдётся простое число p, не входящее в эту группу. С этой целью рассмотрим число $P+1$, где $P=p_1p_2 \ldots p_k$, и обозначим через p наименьший делитель этого

числа, отличный от 1. Очевидно, что p есть простое число; но p не может совпадать ни с одним из чисел $p_1, p_2, \ldots, p_k$, так как p есть делитель числа $P+1$, которое при делении на любое из чисел $p_1, p_2, \ldots, p_k$ даёт в остатке 1 и, следовательно, не делится нацело. Таким образом, p есть новое простое число, не входящее в состав заданной группы, и теорема Евклида доказана.

В вопросе о законах чередования простых чисел в натуральном ряду можно отметить, повидимому, ещё только один факт, доказывающийся столь же просто, как теорема Евклида: *существуют сколь угодно длинные участки натурального ряда, вовсе не содержащие простых чисел* и, следовательно, сплошь состоящие из чисел составных.

В самом деле, если $n>1$ — любое натуральное число, то в ряду чисел

$$n!+2, \quad n!+3, \quad n!+4, \quad \ldots, \quad n!+n$$

(представляющих собой участок натурального ряда длины $n-1$) не может содержаться ни одного простого числа, так как $n!+2$ делится на 2, $n!+3$ — на 3 и т. д., наконец, $n!+n$ делится на n, причём во всех случаях делитель меньше делимого.

Вопрос о распределении простых чисел в натуральном ряду почти совершенно не был продвинут от Евклида до Эйлера. С целью подметить какие-либо закономерности в чередовании простых чисел были составлены таблицы этих чисел, начиная от 2 и до весьма больших пределов (в настоящее время примерно до десяти миллионов). Изучение этих таблиц показывало, что, продвигаясь в натуральном ряду, мы в среднем встречаем простые числа всё реже и реже; но это — только в среднем. Уменьшение количества простых чисел происходит чрезвычайно нерегулярно; после значительных разрежений снова появляются «сгустки», причём до сих пор не установлена закономерность чередования этих сгустков и разрежений.

Это придаёт проблеме распределения простых чисел её исторически известную влекущую силу.

Важнейший из результатов Эйлера в этой области является теоретическим обоснованием этого постепенного уменьшения количества простых чисел во всё более удалённых частях натурального ряда, с которым мы, как уже было сказано, встречаемся при изучении таблиц. Условимся обозначать через $\pi(n)$ число простых чисел, не превышающих числа n, так что, например, $\pi(10)=4$, $\pi(23)=9$ и т. д. Тогда отношение $\pi(n)/n$ (которое, конечно, всегда заключено между нулём и единицею) можно рассматривать как долю, как «среднюю плотность» простых чисел в отрезке натурального ряда от 1 до n. Чем эта дробь меньше, тем меньшая доля натуральных чисел отрезка $(1, n)$ принадлежит множеству простых чисел.

Теорема Эйлера. *При неограниченном возрастании числа n*

$$\frac{\pi(n)}{n} \to 0.$$

Это означает, что во всех достаточно больших начальных отрезках натурального ряда подавляющее большинство чисел будет составным, и лишь ничтожная доля будет входить в совокупность простых чисел.

Чтобы доказать эту теорему Эйлера, нам понадобится предварительно установить следующее вспомогательное предложение:

Лемма. *Пусть* $p_1, p_2, \ldots$ *означают простые числа, расположенные в порядке возрастания* (так что $p_1 = 2$, $p_2 = 3$ и т. д.). *Тогда*

$$\Pi_n = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_n}\right) \to 0$$

при неограниченном возрастании n.

Для доказательства заметим, что для любого k

$$\frac{1}{1 - \frac{1}{p_k}} = 1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \ldots = \sum_{s=0}^{\infty} \frac{1}{p_k^s}.$$

Поэтому

$$\frac{1}{\Pi_n} = \left(\sum_{s=0}^{\infty} \frac{1}{p_1^s}\right)\left(\sum_{s=0}^{\infty} \frac{1}{p_2^s}\right)\ldots\left(\sum_{s=0}^{\infty} \frac{1}{p_n^s}\right).$$

Все n множителей правой части представляют собой абсолютно сходящиеся ряды, которые, как известно[1]), можно перемножать почленно как конечные суммы. Общий член произведения будет иметь вид

$$\frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}},$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — любые числа ряда 0, 1, 2, ... Таким образом, мы можем написать:

$$\frac{1}{\Pi_n} = \sum_{\alpha_1, \alpha_2, \ldots, \alpha_n} \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}},$$

где суммирование производится (в любом порядке) по всем комбинациям чисел $\alpha_1, \alpha_2, \ldots, \alpha_n$. Но в виде $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, при надлежащем выборе чисел α_i, может быть, очевидно, представлено любое

---

[1]) См. Э. э. м. кн. 3, Дифференциальное и интегральное исчисление.

натуральное число, не имеющее других простых делителей, кроме $p_1, p_2, \ldots, p_n$, и, в частности, любое натуральное число, не превосходящее p_n. Таким образом, если $1 \leqslant m \leqslant p_n$, то дробь $\frac{1}{m}$ обязательно найдётся среди слагаемых правой части полученного равенства. Поэтому

$$\frac{1}{\Pi_n} > \sum_{m=1}^{p_n} \frac{1}{m}.$$

Но ряд $\sum_{m=1}^{\infty} \frac{1}{m}$ («гармонический» ряд), как известно, расходится [1]). Поэтому, сколь бы мало ни было положительное число ε, если n (а следовательно, и p_n) достаточно велико, мы будем иметь:

$$\sum_{m=1}^{p_n} \frac{1}{m} > \frac{1}{\varepsilon},$$

и следовательно, в силу предыдущего неравенства

$$\frac{1}{\Pi_n} > \frac{1}{\varepsilon},$$

откуда

$$\Pi_n < \varepsilon.$$

Это неравенство выполняется, таким образом, для всех достаточно больших n, что ввиду произвольной малости числа ε и доказывает лемму.

Переходя теперь к доказательству теоремы Эйлера, мы обозначим через P_n произведение $p_1 p_2 \ldots p_n$ первых n простых чисел.

Для нашей цели важно знать число Q_n чисел ряда

$$1, 2, \ldots, P_n, \tag{3}$$

не делящихся ни на одно из простых чисел $p_1, p_2, \ldots, p_n$. Оказывается, что

$$Q_n = P_n \Pi_n = P_n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right).$$

Подробный вывод этой формулы читатель найдёт в главе II (стр. 282).

Пусть теперь s и r — любые натуральные числа. Тогда, очевидно, для того чтобы число $sP_n + r$ делилось на какое-либо из чисел $p_1, p_2, \ldots, p_n$, необходимо и достаточно, чтобы такою делимостью обладало число r. Поэтому ряд чисел

$$sP_n + 1, \quad sP_n + 2, \ldots, sP_n + P_n = (s+1)P_n$$

[1]) См. предыдущее подстрочное примечание.

при любом $s \geqslant 0$ содержит столько же чисел, не делящихся ни на одно из простых чисел $p_1, p_2, \ldots, p_n$, сколько их имеется в ряду (3), т. е. Q_n.

Если теперь задано сколь угодно малое положительное число ε, то, прежде всего, выберем число n так, чтобы было:

$$\Pi_n = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right) < \varepsilon,$$

что возможно в силу доказанной нами леммы. Если теперь q — любое натуральное число, то пусть оно при делении на P_n даёт в частном s и в остатке r, так что

$$q = sP_n + r \qquad (0 \leqslant r < P_n).$$

Оценим число $\pi(q)$ простых чисел в отрезке $(1, q)$. В число этих простых чисел могут, прежде всего, входить n чисел $p_1, p_2, \ldots, p_n$. Все остальные простые числа отрезка $(1, q)$ не делятся ни на одно из чисел $p_1, p_2, \ldots, p_n$, а потому число их в отрезке $(1, q)$ не превосходит числа тех чисел этого отрезка, которые не делятся ни на одно из чисел $p_1, p_2, \ldots, p_n$. Но таких чисел, как мы уже знаем, имеется в точности $Q_n = P_n\Pi_n$ в каждом из отрезков $(1, P_n)$, $(P_n + 1, 2P_n)$, $(2P_n + 1, 3P_n)$, $\ldots$, $((s-1)P_n + 1, sP_n)$, т. е. в точности $sQ_n = sP_n\Pi_n$ в отрезке $(1, sP_n)$; наконец, в отрезке $(1, q) = (1, sP_n + r)$ их не более чем

$$sQ_n + r < sP_n\Pi_n + P_n.$$

Таким образом,

$$\pi(q) < n + sP_n\Pi_n + P_n,$$

откуда

$$\frac{\pi(q)}{q} < \frac{n + sP_n\Pi_n + P_n}{sP_n + r} \leqslant \frac{n + P_n + sP_n\Pi_n}{sP_n} = \frac{n + P_n}{sP_n} + \Pi_n.$$

Если теперь число q (а следовательно, и s) сделать достаточно большим (сохраняя n неизменным), то первое слагаемое правой части может быть сделано меньшим, нежели ε; а так как $\Pi_n < \varepsilon$ по выбору числа n, то

$$\frac{\pi(q)}{q} < 2\varepsilon$$

для всех достаточно больших q, т. е.

$$\lim_{q \to \infty} \frac{\pi(q)}{q} = 0,$$

и теорема Эйлера доказана.

Этот замечательный результат говорит о том, что простые числа расположены в натуральном ряду в известном смысле «редко» — реже, например, чем члены любой арифметической прогрессии (с как угодно большой разностью). Однако это — только в среднем. У нас

нет никаких оснований представлять себе дело так, будто где-то там, очень далеко в натуральном ряду, каждое простое число стоит в одиночестве, не имея близких соседей ни в ту, ни в другую сторону. Напротив, изучение таблиц показывает, повидимому, что мы от времени до времени всё вновь и вновь встречаем в натуральном ряду очень близких простых соседей, даже так называемых «близнецов», отстоящих друг от друга всего на две единицы, как (5, 7), (41, 43), (101, 103) и т. д. Правда, вопрос о том, существует ли бесчисленное множество таких «близнецов», в настоящее время наукой ещё не решён; у нас, однако, нет никаких оснований считать такое существование невозможным.

Сделаем ещё следующее интересное замечание. Та лемма, которую мы доказали выше, привела нас к теореме Эйлера, говорящей о сравнительной «редкости» расположения простых чисел в натуральном ряду. Но та же самая лемма даёт возможность установить (и притом гораздо более простым путём), что простые числа расположены в натуральном ряду всё же и достаточно густо. В самом деле, из теории бесконечных произведений [1] известно, что стремление к нулю произведения

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)$$

при неограничено возрастающем n равносильно расходимости ряда $\sum_{n=1}^{\infty}\frac{1}{p_n}$, т. е. тому, что сумма

$$\sum_{i=1}^{n}\frac{1}{p_i}$$

неограниченно возрастает с возрастанием n; в этом отношении ряд простых чисел ведёт себя так же, как весь натуральный ряд (расходимость «гармонического» ряда $1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{n}+\dots$), в противоположность, например, ряду «полных квадратов» 1^2, 2^2, 3^2, ... (ряд $\sum_{n=1}^{\infty}\frac{1}{n^2}$ сходится). Это показывает, что простые числа в некотором смысле расположены «гуще», чем полные квадраты.

Все эти элементарно доказуемые факты, установленные примерно к началу XIX столетия, дают, однако, ещё только весьма смутное представление о густоте расположения простых чисел в натуральном ряду. Учёные той эпохи давно уже лелеяли мечту о завоевании гораздо более значительном: найти для функции $\pi(n)$ (число простых

[1] См. А. Я. Хинчин, Восемь лекций по математическому анализу, Гостехиздат, 1948.

чисел, не превосходящих n) хорошее приближённое выражение в виде какой-нибудь простой аналитической функции от n, исследовать рост которой не представляло бы никаких затруднений. Представлялась, например, очень заманчивой мысль найти для функции $\pi(n)$ «асимптотическое» аналитическое выражение, т. е. такую аналитическую функцию $\varphi(n)$, чтобы

$$\frac{\pi(n)}{\varphi(n)} \to 1 \quad (n \to \infty)$$

(иначе говоря, чтобы $\pi(n)$ и $\varphi(n)$ были «эквивалентными» бесконечно большими). Однако наука той эпохи не располагала ещё необходимыми средствами для решения этой важной задачи. Изучение таблиц показывало, что среди элементарных функций имеется одна очень простая, именно $\frac{n}{\ln n}$, дающая (в пределах таблиц) при больших n хорошее приближение для $\pi(n)$, и многие крупнейшие учёные того времени (Лежандр, Гаусс) настойчиво пытались теоретически обосновать эту лишь эмпирически подмеченную близость. Задача оказалась, однако, непомерно трудной, и ни одного результата в этом направлении не удалось получить вплоть до середины XIX столетия, когда замечательные исследования нашего великого учёного П. Л. Чебышева сдвинули, наконец, вопрос с мёртвой точки.

Маячившей перед всеми исследователями целью было, как уже сказано, доказательство соотношения

$$\frac{\pi(n)}{\frac{n}{\ln n}} = \frac{\pi(n)\ln n}{n} \to 1 \qquad (n \to \infty). \tag{4}$$

На пути к этой цели, которая в ту эпоху ещё не могла быть достигнута, Чебышев впервые д о к а з а л несколько важных фактов, среди которых отметим два следующих:

1. Если предел

$$\lim_{n \to \infty} \frac{\pi(n)\ln n}{n}$$

существует, то этот предел равен единице.

2. Для всех достаточно больших n

$$\ln 2 < \frac{\pi(n)\ln n}{n} < 2\ln 2.$$

Значительность этих замечательных достижений, уже довольно близко подводящих нас к окончательной цели (4), в особенности подчёркивается двумя обстоятельствами: во-первых, тем, что до Чебышева в этом направлении не удавалось доказать ровно ничего, так что наш великий математик не имел предшественников и все идеи и методы доказательств должен был создавать совершенно заново; во-вторых, замечательно то, что Чебышев получил свои

важнейшие результаты вполне элементарными арифметическими приёмами, не прибегая к средствам высшей математики.

Вслед за работами Чебышева появилось исследование немецкого математика Римана, указавшего на совершенно новый, сложный аналитический подход к задаче распределения простых чисел. Сам Риман не получил своим методом ни одного арифметического результата. Однако значительно позже, уже в самом конце XIX столетия, метод Римана в связи с развившейся к тому времени теорией функциий комплексной переменной обнаружил замечательную мощность. В частности, в 1894 г. французскому учёному Адамару удалось, наконец, достигнуть давно преследуемой цели — доказать соотношение (4), показывающее, что функция $\frac{n}{\ln n}$ действительно служит асимптотическим выражением для числовой функции $\pi(n)$.

Дальнейшие усилия вплоть до настоящего времени были направлены на уточнение этого результата, т. е. на возможно более точную оценку разности

$$\frac{\pi(n)\ln n}{n} - 1,$$

которая согласно теореме Адамара бесконечно мала при $n \to \infty$. Выдающиеся результаты в этом направлении получены в последние годы советской школой теории чисел, руководимой акад. И. М. Виноградовым, одним из величайших творцов арифметической науки нашей эпохи.

Другая линия развития теории простых чисел, также идущая от теоремы Евклида о бесконечности множества простых чисел, стремится установить существование бесконечного множества простых чисел в той или иной ч а с т и натурального ряда, т. е. среди натуральных чисел того или иного определённого вида. Классическим результатом в этом направлении является теорема Дирихле о существовании бесконечного множества простых чисел в любой арифметической прогрессии, первый член и разность которой взаимно просты. Однако до сих пор наука не смогла продвинуться существенно дальше этого результата (для которого, кстати сказать, мы до сих пор не имеем вполне элементарного доказательства). Теорема Дирихле утверждает, что если числа a и b взаимно просты, то существует бесчисленное множество простых чисел вида $ax + b$ (где x — целое число). Следующим естественным шагом было бы исследование в том же смысле выражений второй степени, т. е. выражений вида $ax^2 + bx + c$. Однако в этом направлении ничего сделать не удалось. Современная наука не знает никакого подхода даже к простейшему частному случаю этой задачи — к вопросу о том, существует ли бесчисленное множество простых чисел среди чисел вида $x^2 + 1$, т. е. в ряду чисел 2, 5, 10, 17, 26, 37, ...

Наконец, особый и очень интенсивно культивируемый круг вопросов теории простых чисел составляют задачи, группирующиеся

около знаменитой проблемы Гольдбаха. Уже давно было замечено, что чётные числа, начиная с 4, повидимому, могут все быть представлены в виде суммы двух простых чисел ($4=2+2$, $6=3+3$, $8=3+5$, $10=3+7$, $12=5+7$ и т. д.), а следовательно, нечётные числа — в виде суммы трёх простых чисел. Проблема Гольдбаха состоит в решении вопроса о том, действительно ли это так для всех чётных (соответственно, нечётных) чисел.

Двадцать лет назад казалось, что наука не знает никакого подхода к этой труднейшей задаче. После бесплодных попыток, продолжавшихся более столетия, замечательный успех в направлении решения проблемы Гольдбаха был достигнут в 1930 г. молодым советским учёным Л. Г. Шнирельманом. Он впервые доказал существование такого постоянного числа k, что всякое натуральное число, кроме 1, может быть представлено в виде суммы не более чем k простых слагаемых. До работы Шнирельмана к этому результату столь же мало умели подойти, как и к самой проблеме Гольдбаха; тем более замечательно, что всё исследование Шнирельмана проведено настолько элементарными арифметическими методами, что могло бы быть в точности в том же виде выполнено и 100 лет назад, в эпоху Чебышева.

Постоянная k, оцениваемая непосредственно по исследованиям Шнирельмана, оказывалась очень большою; многие учёные сейчас же занялись попытками её снижения с помощью столь же элементарных приёмов, и в несколько лет удалось снизить её до 69.

Однако уже в 1936 г. И. М. Виноградов, работая созданным им самим аналитическим методом, полностью доказал гипотезу Гольдбаха для всех достаточно больших нечётных чисел, т. е. показал, что любое достаточно большое нечётное число может быть представлено в виде суммы трёх простых слагаемых; из этого результата непосредственно вытекает, что все достаточно большие чётные числа представляются как суммы четырёх простых слагаемых; таким образом, постоянная k Шнирельмана сразу снижается до 4. Учитывая историческую знаменитость проблемы Гольдбаха и огромное количество потраченных на неё во всём мире усилий, следует признать этот результат И. М. Виноградова одним из крупнейших достижений советской математики.

ГЛАВА II

МЕТОД СРАВНЕНИЙ

§ 4. Введение

Особая трудность, которою во все времена были отмечены задачи теории чисел, заставляла исследователей искать всё новых и новых методов в этой ветви математической науки. И в настоящее время мы имеем в теории чисел такое методологическое многообразие, как, пожалуй, ни в одной другой математической дисциплине. Характерной чертой для всех этих методов является сравнительная ограниченность их приложений; каждый такой метод, как правило, может быть применён к решению лишь более или менее узкого круга родственных между собою задач; как только мы выходим за пределы такого круга, приходится искать новых, подчас весьма инородных методов.

Различные методологические приёмы теории чисел можно разделять по их предметной природе: мы имеем ряд элементарных методов (метод эратосфенова решета, метод алгорифма Евклида и ряд других); но наряду с ними мы имеем и несколько мощных аналитических методов; всё более и более возрастает, наконец, значение методов геометрических, ведущих своё начало от исследований Минковского. С другой стороны, методы эти могут быть различаемы и в другом отношении. В одних из них объединяющим началом служит та или иная предметно-содержательная идея (таков, например, метод «геометрии чисел» Минковского), в основе же других лежит некоторый формальный приём; встречаются, разумеется, и смешанные методологические типы.

Среди формальных элементарно-арифметических методов особое значение приобрёл так называемый *метод сравнений*, созданный Гауссом. На этот метод надо смотреть, как на некий формальный аппарат, не заключающий в себе большого идейного содержания, но представляющий значительную техническую ценность; овладение им позволяет в большом числе случаев со сравнительной лёгкостью получать такие результаты, к которым другие пути обременительно длинны. Вместе с тем простейшие основы теории

сравнений оказались таким формальным инструментом, овладение которым оказывает заметную помощь при решении почти любых задач теории чисел, какими бы содержательно-определёнными методами мы над этими задачами ни работали. Можно поэтому без преувеличения считать теорию сравнений (едва ли не единственным) универсальным методом теории чисел, понимая под этим именно то, что основные положения и приёмы этой теории могут оказать существенную, хотя и чисто формальную помощь почти во всех областях арифметической науки. Без овладения элементами этой теории работа в любой области теории чисел была бы в известной мере обречена на отсталый, «кустарный» научный стиль. Однако не надо вместе с тем и преувеличивать значения теории сравнений: даже самое полное овладение её методом вооружает исследователя только технически, не давая ему ещё почти никаких руководящих идей.

В этой главе мы дадим краткий по необходимости очерк основных положений теории сравнений и её простейших приложений. Непревзойдённое по полноте и глубине изложение этой теории читатель может найти в классическом труде П. Л. Чебышева «Теория сравнений» [1]).

§ 5. Сравнения и их основные свойства

Идея сравнения имеет своим основанием то простое замечание, что два числа a и b, дающих при делении на натуральное число m один и тот же остаток, в вопросах делимости обнаруживают по отношению к числу m целый ряд одинаковых свойств. Самое важное из этих свойств состоит в том, что всякий общий делитель чисел a и m будет вместе с тем и общим делителем чисел b и m, и обратно. В частности, наибольший общий делитель (a, m) чисел a и m совпадает с наибольшим общим делителем (b, m) чисел b и m.

В самом деле, если, как предположено, a и b дают при делении на m один и тот же остаток r, то

$$a = km + r, \quad b = lm + r,$$

так что разность

$$a - b = (k - l)\, m$$

делится на m. Отсюда

$$a = qm + b, \quad b = a - qm;$$

эти соотношения и показывают непосредственно, что всякий общий делитель чисел m и b является вместе с тем и делителем числа a, и обратно.

---

[1]) П. Л. Чебышев, Полное собрание сочинений, т. I, Теория чисел, Издательство АН СССР, 1944.

Это общее свойство чисел a и b, вытекающее из их «равноостаточности» при делении на m, оказывается настолько важным, что представляется целесообразным формально зафиксировать такую равноостаточность, придавая ей особое наименование и особое обозначение. Принято называть числа a и b, дающие одинаковые остатки при делении на m, *сравнимыми по модулю* m и обозначать это так:

$$a \equiv b \pmod{m}.$$

Например, $3 \equiv -17 \pmod{5}$.

Сравнимость (т. е. равноостаточность) двух чисел по данному модулю m делает их, как мы видели, в какой-то мере родственными, сходными между собою в их отношении к числу m. Отношение сравнимости есть, таким образом, некое сходство, подобие двух чисел, и установление и использование важнейших свойств этого родственного отношения двух чисел и составляют собою руководящую идею теории сравнений. Надо только твёрдо помнить, что понятие сравнимости всегда связано с определённым модулем, так что то родство или подобие двух чисел, о котором здесь идёт речь, свойственно этим числам не самим по себе, а лишь в их отношении к числу m. Два числа, сравнимые между собою по модулю m, вообще говоря, не будут иметь друг с другом ничего общего по другому модулю m'.

При определении сравнимости двух чисел требование равноостаточности может быть заменено равносильным ему, но более удобным для проверки в конкретных случаях требованием, чтобы разность двух данных чисел делилась на модуль. Так, в только что приведённом примере нет, разумеется, надобности находить остатки чисел 3 и -17 при делении на 5; достаточно убедиться, что разность этих двух чисел $3-(-17)=20$ делится на 5.

Следующие основные теоремы показывают, что со сравнениями можно в значительной мере оперировать, как с обычными равенствами.

Теорема 1. *Сравнения по одному и тому же модулю можно почленно складывать, вычитать и перемножать.*

Пусть

$$\left.\begin{aligned} a &\equiv b \pmod{m}, \\ a' &\equiv b' \pmod{m}. \end{aligned}\right\} \tag{1}$$

Требуется доказать, что

$$a \pm a' \equiv b \pm b' \pmod{m},$$
$$aa' \equiv bb' \pmod{m}.$$

Из (1) вытекает:

$$a - b = mq,$$
$$a' - b' = mq',$$

откуда

$$(a \pm a') - (b \pm b') = (a - b) \pm (a' - b') = m(q - q'),$$

и следовательно,

$$a \pm a' \equiv b \pm b' \pmod{m}.$$

Далее,

$$aa' - bb' = a(a' - b') + b'(a - b) = (aq' + b'q)m,$$

и следовательно,

$$aa' \equiv bb' \pmod{m},$$

что и требовалось доказать.

Примечание. В частности, к обеим частям сравнения можно прибавить одно и то же число, и обе части сравнения можно умножить на одно и то же число.

Мы доказали теорему 1 в предположении двух сравнений. Однако, разумеется, она автоматически распространяется от двух на три, от трёх на четыре и вообще от n на $n+1$ сравнений, так что в силу принципа полной индукции мы можем считать её установленной для любого числа сравнений.

Следствие. *Если*

$$a \equiv b \pmod{m}, \tag{2}$$

то

$$a^k \equiv b^k \pmod{m},$$

где k — любое натуральное число или нуль.

Для доказательства достаточно почленно перемножить k тождественных между собою сравнений (2).

Комбинируя друг с другом полученные нами до сих пор результаты, мы, очевидно, приходим к следующему важному выводу:

Теорема 2. *Пусть $P(x)$ — любой многочлен с целыми коэффициентами. Тогда из*

$$x \equiv y \pmod{m}$$

следует:

$$P(x) \equiv P(y) \pmod{m}.$$

Это предложение представляет большой интерес и для школьного курса арифметики, так как оно служит теоретическим основанием для вывода наиболее важных признаков делимости. Если в десятичной системе число n изображается, считая слева направо, цифрами $a, b, c, \ldots, k, l$, то

$$n = a \cdot 10^s + b \cdot 10^{s-1} + c \cdot 10^{s-2} + \ldots + k \cdot 10 + l.$$

Но

$$10 \equiv 1 \pmod{3} \quad \text{и} \quad \pmod{9};$$

поэтому в силу теоремы 2

$$n \equiv a + b + c + \ldots + k + l \pmod 3 \quad \text{и} \quad \pmod 9,$$

т. е. по модулям 3 и 9 каждое число сравнимо с суммой своих цифр. Но отсюда следует, что наибольший общий делитель с числом 3 (или 9) число n имеет тот же, что и сумма его цифр. В частности, n делится на 3 (или 9) тогда и только тогда, если на это число делится сумма его цифр. Подобным же образом сравнение

$$10 \equiv -1 \pmod{11}$$

в силу теоремы 2 даёт:

$$n \equiv (-1)^s a + (-1)^{s-1} b + \ldots - k + l \pmod{11},$$

откуда непосредственно вытекает известный признак делимости на 11.

Теорема 1, устанавливающая ничем не ограниченную возможность почленного сложения, вычитания и умножения сравнений, ничего не говорит нам о четвёртом арифметическом действии — делении. В частности, мы не знаем ещё, всегда ли возможно деление обеих частей сравнения на одно и то же число (при условии, конечно, что такое деление может быть выполнено без остатка). Мы не случайно отложили рассмотрение этого вопроса; дело в том, что здесь мы впервые встречаемся с таким положением, когда сравнения ведут себя несколько иначе, чем равенства; теперь мы должны подробно разобраться в этом вопросе.

Прежде всего простые примеры легко показывают, что деление, о котором идёт речь, не всегда возможно. Так,

$$45 \equiv 27 \pmod 6;$$

обе части сравнения делятся на 9; однако, выполняя это деление, мы пришли бы к неверному сравнению

$$5 \equiv 3 \pmod 6.$$

Рассмотрим теперь вопрос в общем виде. Пусть

$$a \equiv b \pmod m, \tag{2}$$

причём a и b делятся на одно и то же число d, так что

$$a = da', \quad b = db'.$$

Спрашивается, при каких условиях сравнение (2) можно «сократить» на d, т. е. при каких условиях из (2) следует:

$$a' \equiv b' \pmod m?$$

Сравнение (2) означает, что разность $a - b = d(a' - b')$ делится на m; при каких условиях из этого будет следовать, что и разность

$a' - b'$ должна делиться на m? На этот вопрос отвечает нам теорема 2 главы I: это будет всегда, если числа d и m взаимно просты. Отсюда следует важное правило: *обе части сравнения всегда можно разделить на одно и то же число, взаимно простое с модулем.* Напротив, если число d не взаимно просто с модулем m, то деление обеих частей сравнения на d, вообще говоря, невозможно, как этому учит вышеприведённый пример, где деление привело к неверному результату именно потому, что мы делили на число 9, не взаимно простое с модулем 6.

Обнаруженное нами различие в поведении сравнений и равенств имеет своей причиной то весьма важное обстоятельство, что сравнения, вообще говоря, не подчиняются одному из основных принципов теории равенств: *если произведение двух чисел равно нулю, то по меньшей мере один из сомножителей также равен нулю.* В теории сравнений аналогичный принцип, очевидно, гласил бы: если произведение двух чисел сравнимо с нулём по модулю m, то по меньшей мере один из сомножителей также сравним с нулём по модулю m. Но сравнимость с нулём по модулю m есть не что иное, как делимость на m; поэтому наш принцип гласил бы: если произведение двух чисел делится на m, то по меньшей мере один из сомножителей должен делиться на m. Это же, вообще говоря, неверно: $4 \times 15 = 60$ делится на 6, между тем как ни 4, ни 15 на 6 не делятся. Именно незаконное применение этого принципа, как легко видеть, и привело нас в нашем предыдущем примере к неправильному результату.

Однако теорема 3 главы I учит нас, что есть один случай, когда этот принцип всё же оказывается верным: если модуль p есть простое число, то из делимости на p произведения двух чисел обязательно вытекает делимость на p по меньшей мере одного из сомножителей. Этот замечательный факт имеет своим следствием то, что сравнения по простому модулю в значительно большей степени аналогичны равенствам, нежели сравнения по модулю составному.

В частности, в известном смысле можно сказать, что вопрос о возможности деления обеих частей сравнения на одно и то же число в случае простого модуля решается в точности так же, как для равенств. В самом деле, выше мы убедились, что обе части сравнения всегда можно делить на одно и то же число d, взаимно простое с модулем m; но если m есть число простое, то «быть взаимно простым с m» означает просто «не делиться на m», или, что то же, «не быть сравнимым с нулём по модулю m». Таким образом, в случае простого модуля запрещается делить обе части сравнения лишь на такие числа, которые сравнимы с нулём по данному модулю. Но числам, сравнимым с нулём по данному модулю, в теории равенств по аналогии соответствует обыкновенный нуль, деление на который ведь также запрещается. Таким образом, мы

видим, что в этом вопросе, как и во многих других, сравнения по простому модулю ведут себя в точности аналогично равенствам. Что касается сравнений по составному модулю, то здесь мы, напротив, наблюдаем существенно иные закономерности, нежели в теории равенств.

§ 6. Классификация чисел по данному модулю

Мы назвали два числа сравнимыми по модулю m, если они дают одинаковые остатки при делении на m; отсюда непосредственно следует, что если каждое из двух чисел a и b сравнимо по модулю m с одним и тем же числом c, то и $a \equiv b \pmod m$. А это обстоятельство позволяет нам в свою очередь объединить все числа, сравнимые с данным числом a (а значит, и сравнимые между собой) по модулю m, в один к л а с с. Таким образом, все целые числа распадаются на к л а с с ы п о м о д у л ю m; все числа одного и того же класса сравнимы между собою по модулю m, но два числа разных классов никогда по модулю m не сравнимы друг с другом.

Как число и взаимоотношения классов, так и внутренняя структура их очень легко обозримы. Все числа одного и того же класса дают при делении на модуль m один и тот же остаток. Но остатками при делении на m могут быть только следующие m чисел:

$$0,\ 1,\ 2,\ \ldots,\ m-1.$$

Следовательно, число классов по модулю m равно m. Класс, характеризуемый данным остатком $r\ (0 \leqslant r \leqslant m-1)$, образуют числа вида $mx+r$, где x — любое целое число; очевидно, эти числа образуют бесконечную в обоих направлениях арифметическую прогрессию с разностью m. Таким образом, разбиение множества всех целых чисел на классы по модулю m есть просто разбиение этого множества на m арифметических прогрессий с разностью m.

Если мы произвольным образом выберем по одному числу в каждом из классов, то мы будем иметь группу из m чисел, характеризуемую тем, что никакие два числа этой группы не сравнимы между собою по модулю m и что, с другой стороны, любое целое число сравнимо по модулю m с одним из чисел выбранной группы. Такую группу чисел называют *полной системой вычетов* по модулю m. Очевидно, что таких полных систем вычетов по любому модулю существует бесчисленное множество. Так, полной системой вычетов по модулю 3 может служить любая из троек чисел (0, 1, 2), (10, 11, 12), (— 4, 6, — 5), и бесчисленное множество других.

Так как во многих вопросах теории делимости числа одного и того же класса могут, как мы знаем, заменять друг друга, то в вопросах подобного рода обычно бывает безразлично, какую из бесчисленного множества полных систем вычетов мы изберём для нашего рассуждения; это обстоятельство создаёт такой элемент про-

извола, которым часто удаётся воспользоваться для упрощения расчётов (например, для замены больших чисел значительно меньшими).

В теоретических применениях понятия полной системы вычетов важную роль играет следующая

Теорема 3. *Если числа a и m взаимно просты и в выражении $ax+b$ число x пробегает полную систему вычетов по модулю m, то и получаемые значения этого выражения образуют полную систему вычетов по модулю m.*

Так как число получаемых значений выражения $ax+b$ равно m, то для того, чтобы убедиться, что они образуют полную систему вычетов по модулю m, достаточно показать, что все они принадлежат разным классам по модулю m. Но если бы для каких-либо двух чисел x_1 и x_2, принадлежащих разным классам по модулю m, мы имели

$$ax_1+b\equiv ax_2+b \pmod m.$$

то отсюда следовало бы:

$$ax_1\equiv ax_2 \pmod m;$$

так как a взаимно просто с m, то, как мы знаем, обе части сравнения можно разделить на a; это даёт:

$$x_1\equiv x_2 \pmod m,$$

что неверно. Таким образом, теорема 3 доказана. Скоро мы встретимся с её важными применениями.

Мы уже знаем, что все числа, принадлежащие одному и тому же классу, имеют с модулем одних и тех же общих делителей и, значит, — одного и того же наибольшего общего делителя. В частности, если одно из чисел данного класса взаимно просто с модулем, то так же обстоит дело и для всех чисел данного класса. Мы можем поэтому говорить о классах, взаимно простых с модулем. Группа чисел, содержащая по одному представителю от каждого класса, взаимно простого с модулем, называется *приведённой* (в отличие от полной) системой вычетов по данному модулю. Самый простой способ получить приведённую систему вычетов по модулю m состоит, очевидно, в том, чтобы отобрать в ряду чисел

$$1,\ 2,\ \ldots,\ m,$$

представляющих собою полную систему вычетов по модулю m, те, которые взаимно просты с m. Таким образом, число классов, взаимно простых с m (или, что то же, число членов любой приведённой системы вычетов по модулю m), равно числу натуральных чисел, не превосходящих m и взаимно простых с m. Это число, зависящее, очевидно, только от m, и обозначаемое через $\varphi(m)$, есть одна из важнейших арифметических функций натурального числа m. Мы увидим дальше, как просто может быть найдено значение этой функции, если известно разложение числа m на простые множители.

Для приведённой системы вычетов имеет место следующее важное предложение, аналогичное теореме 3 для полной системы вычетов:

Теорема 4. *Если числа a и m взаимно просты и если в выражении ax число x пробегает какую-либо приведённую систему вычетов по модулю m, то и получаемые значения этого выражения образуют приведённую систему вычетов по модулю m.*

Следует обратить внимание на то, что фигурирующее в теореме 3 произвольное число b в теореме 4 обязательно равно нулю; это показывает, что свойство полных систем, выражаемое теоремой 3, значительно шире того свойства приведённых систем, которое выражается теоремой 4.

Для доказательства теоремы 4 достаточно заметить, что, когда x пробегает какую-либо приведённую систему вычетов по модулю m, получающиеся при этом $\varphi(m)$ значений произведения ax все взаимно просты с m и, как было показано при доказательстве теоремы 3, все принадлежат различным классам по модулю m.

Теорема 4 позволяет легко доказать одно интересное и важное предложение, найденное Эйлером. Пусть числа a и m взаимно просты и пусть

$$r_1, r_2, \ldots, r_s, \tag{3}$$

где для краткости положено $\varphi(m) = s$, — любая приведённая система вычетов по модулю m. В силу теоремы 4 числа

$$ar_1, ar_2, \ldots, ar_s \tag{4}$$

также представляют собою приведённую систему вычетов по модулю m. Таким образом, каждое из чисел (4) сравнимо по модулю m с одним из чисел (3), т. е.

$$\left.\begin{aligned} ar_1 &\equiv r_{i_1} \\ ar_2 &\equiv r_{i_2} \\ &\cdots\cdots \\ ar_s &\equiv r_{i_s} \end{aligned}\right\} \pmod m,$$

где ряд индексов $i_1, i_2, \ldots, i_s$ есть расположенный только в другом порядке ряд чисел $1, 2, \ldots, s$. Перемножая эти сравнения почленно, мы находим:

$$a^{\varphi(m)} r_1 r_2 \ldots r_s \equiv r_{i_1} r_{i_2} \ldots r_{i_s} \equiv r_1 r_2 \ldots r_s \pmod m.$$

Так как каждое r_i взаимно просто с m, то и произведение их взаимно просто с m, и, следовательно, мы можем разделить на это произведение обе части последнего сравнения. Это и приводит нас к теореме Эйлера, утверждающей, что *если a взаимно просто с m, то*

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Пример. $\varphi(10)=4$; $3^4=81\equiv 1 \pmod{10}$; $7^4=2401\equiv \equiv 1 \pmod{10}$.

В частном случае, когда модулем служит простое число p, в ряду 1, 2, ..., p взаимно простыми с p будут все числа, кроме p; таким образом, $\varphi(p)=p-1$; соответствующий случай теоремы Эйлера был ранее доказан Ферма́.

Теорема Ферма́. *Если p — простое число и a не делится на p, то*

$$a^{p-1}\equiv 1 \pmod{p}.$$

Примечание. Это предложение часто называют «малой теоремой Ферма» в отличие от так называемой «великой теоремы Ферма» о невозможности решения в целых положительных числах уравнения $x^n+y^n=z^n$ при целом $n>2$ (это утверждение, доказательством которого Ферма, по его свидетельству, обладал, как известно, не доказано до настоящего времени). Если измерять важность той или другой теоремы её ролью и значением в развитии данной отрасли науки, то следовало бы, пожалуй, принять обратную терминологию. Если «великая» теорема когда-либо будет доказана, то сам этот факт, насколько здесь возможно предвидение, не даст науке никакой опорной точки для значительных новых достижений и, по всей вероятности, останется более или менее изолированным. Напротив, установленная нами «малая» теорема уже давно стала важнейшим орудием исследования и притом не только в теории целых чисел, но и в значительно более широких областях арифметики и алгебры.

Мы переходим теперь к установлению вида функции $\varphi(m)$, означающей число натуральных чисел, не превосходящих m и взаимно простых с m.

Прежде всего мы докажем, что *если числа m и n взаимно просты, то*

$$\varphi(mn)=\varphi(m)\varphi(n).$$

Чтобы подсчитать $\varphi(mn)$, удобно расположить натуральные числа от 1 до mn в следующую таблицу:

1	2 ...	k ...	m
$m+1$	$m+2$ ...	$m+k$ ...	$2m$
$2m+1$	$2m+2$ ...	$2m+k$ ...	$3m$
. . . . .	. . . . .	. . . . .	. .
$(n-1)m+1$	$(n-1)m+2$ ...	$(n-1)m+k$ ...	nm

и постараться определить, сколько эта таблица содержит чисел, взаимно простых с произведением mn. Но для того, чтобы быть

взаимно простым с произведением mn, число должно быть взаимно простым как с m, так и с n. Поэтому мы можем наш подсчёт вести так: сначала отобрать из таблицы все числа, взаимно простые с m, а потом уже из них выбрать те, которые взаимно просты и с n. Так мы и поступим.

В нашей таблице, очевидно, все числа, стоящие в одном столбце, принадлежат одному классу по модулю m и, значит, либо все взаимно просты с m, либо все не взаимно просты. Мы можем поэтому говорить о «столбцах, взаимно простых с m». Число таких столбцов проще всего определить, подсчитывая, сколько чисел, взаимно простых с m, содержит верхняя строка нашей таблицы 1, 2, ..., m. Очевидно, таких чисел будет $\varphi(m)$, и под каждым из них лежит столбец чисел, взаимно простых с m.

Выберем теперь любой из этих $\varphi(m)$ столбцов, например

$$k,\ m+k,\ 2m+k,\ \ldots,\ (n-1)m+k, \tag{5}$$

и подсчитаем, сколько в нём будет чисел, взаимно простых с n. Числа этого столбца представляют собою значения выражения $mx+k$, когда x пробегает ряд чисел 0, 1, 2, ..., $n-1$, т. е. полную систему вычетов по модулю n. Так как m взаимно просто с n, то в силу теоремы 3 числа (5) также образуют полную систему вычетов по модулю n; но любая полная система вычетов по модулю n содержит в точности $\varphi(n)$ чисел, взаимно простых с n; итак, любой столбец нашей таблицы содержит $\varphi(n)$ чисел, взаимно простых с n.

Резюмируем: наша таблица содержит $\varphi(m)$ столбцов, взаимно простых с m, и в каждом из этих столбцов имеется $\varphi(n)$ чисел, взаимно простых с n; таким образом, таблица содержит $\varphi(m)\varphi(n)$ чисел, взаимно простых как с m, так и с n; но это и будут числа, взаимно простые с произведением mn, так что действительно

$$\varphi(mn)=\varphi(m)\varphi(n),$$

что и требовалось доказать.

Теперь уже легко найти общее выражение для функции $\varphi(m)$. Пусть разложение числа m на простые множители имеет вид

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r},$$

где $p_1,\ p_2,\ \ldots,\ p_r$ — различные между собой простые числа, а $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_r$ — любые натуральные числа. Тогда согласно только что доказанному свойству функции $\varphi(m)$

$$\varphi(m)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_r^{\alpha_r}). \tag{6}$$

Но $\varphi(p_i^{\alpha_i})\ (1\leqslant i\leqslant r)$ есть число натуральных чисел, не превосходящих $p_i^{\alpha_i}$ и взаимно простых с $p_i^{\alpha_i}$, т. е. просто не делящихся

на p_i; чтобы подсчитать это число, заметим, что в ряду чисел

$$1, 2, \ldots, p_i^{\alpha_i}$$

кратными p_i будут числа

$$p_i, 2p_i, 3p_i, \ldots, p_i^{\alpha_i - 1} p_i = p_i^{\alpha_i},$$

т. е. всего $p_i^{\alpha_i - 1}$ чисел. Остальные

$$p_i^{\alpha_i} - p_i^{\alpha_i - 1}$$

чисел этого ряда и будут не делящимися на p_i, т. е. взаимно простыми с $p_i^{\alpha_i}$; таким образом,

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right).$$

Поэтому соотношение (6) даёт нам:

$$\varphi(m) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right)p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \ldots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) =$$
$$= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right).$$

Эта формула и решает поставленную нами задачу. Интересно отметить, что выражение, полученное нами для $\varphi(m)$, не зависит явным образом от чисел α_i, так что для вычисления $\varphi(m)$ нет надобности знать те показатели, с которыми различные простые числа входят в выражение m: достаточно знать только сами эти простые числа.

Пример.

$$120 = 2^3 \cdot 3 \cdot 5;$$

$$\varphi(120) = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 120 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 32.$$

Заметим еще, что на стр. 265 главы I нам нужно было найти число Q_n натуральных чисел от 1 до $P_n = p_1 p_2 \ldots p_n$, не делящихся ни на одно из простых чисел $p_1, p_2, \ldots, p_n$. Очевидно, что это число есть не что иное, как $\varphi(P_n)$; и формула для Q_n, которую мы там привели без доказательства, очевидно, представляет собою частный случай полученной нами теперь общей формулы.

§ 7. Сравнения, содержащие неизвестные

Подобно тому как мы делим равенства на тождества и уравнения, мы можем, конечно, и среди сравнений различать тождественные (т. е. такие, которые либо вовсе не содержат букв, либо выполняются при любых значениях входящих в них букв) и содержащие неизвестные (т. е. содержащие такие буквы, значения которых

должны быть специально выбраны для того, чтобы сравнение удовлетворилось). Примерами тождественных сравнений могут служить:

$$103 \equiv 1 \pmod{17}, \quad (a+b)^2 \equiv a^2 \pmod{b}.$$

Примером сравнения, содержащего неизвестное, может служить:

$$x^2 + 1 \equiv 0 \pmod{10}.$$

Мы будем здесь говорить только о сравнениях с одним неизвестным. Такое сравнение называется *алгебраическим степени n*, если оно имеет вид

$$P(x) \equiv 0 \pmod{m},$$

где $P(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$ — многочлен степени n с целыми коэффициентами, причём $a_0 \not\equiv 0 \pmod{m}$ (т. е. a_0 не делится на модуль), подобно тому как от алгебраического уравнения степени n мы требуем, чтобы коэффициент при x^n не равнялся нулю.

В силу теоремы 2 мы непосредственно видим, что если число x_0 удовлетворяет некоторому алгебраическому сравнению по модулю m, то и любое число x, сравнимое с x_0 по модулю m, также будет ему удовлетворять. Для алгебраических сравнений, таким образом, характерно, что корни их образуют целые классы по данному модулю; поэтому обычно *решением* алгебраического сравнения по модулю m принято называть не отдельное число, а целый класс (по модулю m) чисел, удовлетворяющих данному сравнению. Соответственно этому под числом решений данного алгебраического сравнения по модулю m понимают не число чисел, ему удовлетворяющих (таких чисел всегда имеется либо ни одного, либо бесконечное множество), а число классов по модулю m, состоящих из удовлетворяющих ему чисел.

Мы, прежде всего, подробно рассмотрим наиболее важный случай линейных сравнений (т. е. сравнений первой степени) с одним неизвестным, общий вид которых

$$ax \equiv b \pmod{m}. \tag{7}$$

Если число a взаимно просто с модулем m, то при пробегании x полной системы вычетов по этому модулю соответствующие значения произведения ax в силу теоремы 3 будут представлять собой полную систему вычетов по модулю m, так что одно и только одно из этих значений будет сравнимо с b. Наше сравнение имеет, таким образом, в этом случае в точности одно решение аналогично уравнению первой степени с одним неизвестным.

Один из возможных способов фактического нахождения этого решения даёт нам теорема Эйлера: так как

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

то

$$ba^{\varphi(m)} \equiv b \pmod{m},$$

и мы непосредственно видим, что число $ba^{\varphi(m)-1}$ удовлетворяет сравнению (7); так как единственность решения уже установлена, то полное решение сравнения (7) даётся формулой

$$x \equiv ba^{\varphi(m)-1} \pmod{m}. \tag{8}$$

Очевидно, рассматриваемый нами частный случай всегда имеет место, если m есть простое число. В самом деле, число a, которое по самому определению степени сравнения не должно делиться на m, будет при этом условии взаимно просто с m; таким образом, *сравнение первой степени по простому модулю всегда имеет в точности одно решение*, даваемое в силу теоремы Ферма́ формулой

$$x \equiv ba^{m-2} \pmod{m} \tag{9}$$

[надо только иметь в виду, что практически отыскание решений с помощью формул (8) или (9) в большинстве случаев не является кратчайшим путём к цели; кратчайший путь даётся алгорифмом Евклида, см. главу III]. Мы видим, что и в этом вопросе сравнения по простому модулю подчиняются законам, вполне аналогичным соответствующим законам теории уравнений.

Решениями сравнения (7) служат числа x, для которых разность $ax - b$ делится на m, т. е. имеет вид my, где y — также целое число. Поэтому задача решения сравнения (7) равносильна задаче решения в целых числах x, y уравнения

$$ax - b = my,$$

или, что то же,

$$ax - my = b. \tag{10}$$

Это есть общий вид уравнения первой степени с двумя неизвестными. Мы видим, таким образом, что все результаты теории сравнений первой степени с одним неизвестным могут быть истолкованы и вне теории сравнений как законы «неопределённого» или «диофантова» анализа (т. е. учения о решении уравнений в целых числах) первой степени с двумя неизвестными. В частности, основной полученный нами результат может, очевидно, быть сформулирован следующим образом:

Если числа a и m взаимно просты, то уравнение (10) *всегда может быть решено в целых числах; если (x_0, y_0) есть одно из его решений, то все решения даются формулами*

$$x = x_0 + mk, \quad y = y_0 + ak,$$

где k — любое целое число.

В частности, при $b = 1$ задача решения уравнения (10) (при взаимно простых a и m) уже рассматривалась нами в главе I. Там мы доказали (теорема 1) существование решения методом Гаусса. Теперь мы имеем второе доказательство той же тео-

ремы [1]). Это новое доказательство удовлетворительнее прежнего, так как оно не только доказывает существование решения, но даёт метод фактического получения всех решений уравнения (10). Метод этот, однако, не является, как мы уже заметили, кратчайшим из возможных; и в следующей главе мы в третий раз вернёмся к этой задаче, чтобы дать уже практически наилучшее её решение.

Обратимся теперь к случаю, когда наибольший общий делитель d чисел a и m больше 1:

$$(a,\ m)=d>1.$$

Пусть $a=da'$, $m=dm'$, так что $(a',\ m')=1$ (т. е. числа a' и m' взаимно просты). Если b не делится на d, то, как легко видеть, сравнение (7) вовсе не может иметь решений. В самом деле, если какое-нибудь число x удовлетворяет этому сравнению, то

$$ax-b=my,\quad b=ax-my=d(a'x-m'y),$$

т. е. b должно быть кратно d. Если же b делится на d, то пусть $b=db'$; делимость $ax-b=d(a'x-b')$ на $m=dm'$ равносильна делимости $a'x-b'$ на m', т. е. сравнение (7) равносильно сравнению

$$a'x\equiv b'\pmod{m'}.$$

Но это последнее сравнение, в котором $(a',\ m')=1$, имеет, как мы уже знаем, в точности одно решение по модулю m'; другими словами, числа, удовлетворяющие сравнению (7), в рассматриваемом случае образуют один класс по модулю $m'=\frac{m}{d}$; но легко видеть, что один класс по модулю m' распадается на d классов по модулю m; в самом деле, если этот класс по модулю m' записать в виде $x_0+m'z$, где z — любое целое число, то, очевидно, числа этого класса

$$x_0,\ x_0+m',\ x_0+2m',\ \ldots,\ x_0+(d-1)m'$$

будут все разных классов по модулю m, дальше же пойдут повторения:

$$x_0+dm'=x_0+m\equiv x_0\pmod{m},$$

$$x_0+(d+1)m'=x_0+m+m'\equiv x_0+m'\pmod{m},$$

и т. д. Согласно принятой нами терминологии мы должны сказать, что в этом случае сравнение (7) имеет d решений.

Таким образом, вопрос о числе решений сравнения (7) первой степени с одним неизвестным нами теперь разобран до конца. Общий

---

[1]) То обстоятельство, что это новое доказательство содержит ссылку на теорему 2 гл. I, не создаёт, конечно, ложного круга, так как в гл. I мы показали (стр. 261), что теорема 2 может быть доказана независимо от теоремы 1.

результат может быть формулирован в виде следующего простого предложения:

Теорема 5. *Пусть в сравнении* (7) $(a, m)=d$. *Тогда это сравнение имеет d решений, если b делится на d, и ни одного решения в противном случае.*

При этом рассмотренный нами ранее случай $d=1$ полностью укладывается в эту общую формулировку, не требуя никаких оговорок.

Очевидно, мы можем формулировать полученный общий результат и в терминах уравнений первой степени с двумя неизвестными.

Пусть в уравнении

$$ax - my = b$$

$(a, m)=d$. *Тогда, если b делится на d, то данное уравнение имеет бесчисленное множество целых решений, причём если* (x_0, y_0) *есть одно решение, то все решения содержатся в формулах*

$$x = x_0 + k\frac{m}{d}, \quad y = y_0 + k\frac{a}{d}.$$

Если же b не делится на d, то данное уравнение вовсе не имеет целых решений.

Переходя теперь к алгебраическим сравнениям высших степеней, мы ограничимся рассмотрением лишь сравнений по простому модулю p, так как только для них аналогия с уравнениями может быть проведена сколько-нибудь далеко. Таким образом, мы будем иметь дело со сравнениями вида

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{p}, \qquad (11)$$

где p — простое число и a_0 не делится на p.

Прежде всего мы докажем для таких сравнений предложение, аналогичное так называемой «теореме Безу» для алгебраических уравнений.

Теорема 6. *Если* $x \equiv a \pmod{p}$ *есть решение сравнения* (11), *то существует такой многочлен* $Q(x)$ *степени* $n-1$ *с целыми коэффициентами, что тождественно* (т. е. для любого целого x)

$$P(x) \equiv (x-a)\,Q(x) \pmod{p}. \qquad (12)$$

Доказательство этой теоремы легко проводится в точной аналогии с обычным доказательством теоремы Безу. Обычное алгебраическое деление многочлена $P(x)$ на двучлен $x-a$ даёт в частном некоторый многочлен $Q(x)$ степени $n-1$ с целыми коэффициентами и в остатке некоторое целое число r, так что тождественно

$$P(x) = (x-a)\,Q(x) + r.$$

Полагая $x=a$, находим:

$$r=P(a)\equiv 0 \pmod p;$$

поэтому мы имеем тождественно

$$P(x)\equiv (x-a)\,Q(x) \pmod p,$$

что и требовалось доказать.

Если, кроме решения $x\equiv a \pmod p$, сравнение (11) имеет ещё отличное от него решение $x\equiv b \pmod p$, то, полагая в сравнении (12) $x=b$, мы находим:

$$(b-a)\,Q(b)\equiv 0 \pmod p;$$

но $b-a$ не делится на d, так как b по условию есть решение сравнения (11), отличное от a; следовательно,

$$Q(b)\equiv 0 \pmod p,$$

т. е $x\equiv b \pmod p$ есть решение сравнения $Q(x)\equiv 0 \pmod p$, а значит, в силу теоремы 6 тождественно

$$Q(x)\equiv (x-b)\,R(x) \pmod p, \tag{13}$$

где $R(x)$ — многочлен степени $n-2$ с целыми коэффициентами. Из (12) и (13) следует тождественно

$$P(x)\equiv (x-a)(x-b)\,R(x) \pmod p.$$

Продолжая этот процесс, мы, очевидно, приходим к следующему общему выводу: если сравнение (11) имеет $k\leqslant n$ различных решений $x\equiv x_i \pmod p (1\leqslant i\leqslant k)$, то имеет место тождественное сравнение

$$P(x)\equiv (x-x_1)(x-x_2)\ldots(x-x_k)\,L(x) \pmod p,$$

где $L(x)$ — многочлен степени $n-k$ с целыми коэффициентами. Заметим, кстати, что коэффициенты старших членов в многочленах $P(x)$, $Q(x)$, $R(x)$ и $L(x)$ все равны a_0, ибо каждый из этих многочленов есть частное от деления предыдущего многочлена на двучлен вида $x-a$. Этот результат немедленно приводит к следующему важному выводу:

Теорема 7. *Сравнение степени n по простому модулю не может иметь более n решений.*

В самом деле, если бы сравнение (11) имело $n+1$ различных решений $x\equiv x_i \pmod p (1\leqslant i\leqslant n+1)$, то в силу только что проведённого общего рассуждения мы, полагая $k=n$, имели бы тождественно:

$$P(x)\equiv a_0(x-x_1)(x-x_2)\ldots(x-x_n) \pmod p.$$

Полагая здесь $x=x_{n+1}$ и пользуясь тем, что $P(x_{n+1})\equiv 0 \pmod p$, мы нашли бы:

$$a_0(x_{n+1}-x_1)(x_{n+1}-x_2)\ldots(x_{n+1}-x_n)\equiv 0 \pmod p,$$

что невозможно, так как ни один из множителей левой части не может делиться на p.

Это важное предложение, весьма сближающее теорию алгебраических сравнений по простому модулю с теорией алгебраических уравнений, теряет силу в случае составного модуля: мы уже видели, что сравнение первой степени по составному модулю может иметь более одного решения.

Теорема Ферма даёт нам очень ценный пример такого типа сравнений, число решений которых всегда равно показателю степени. В самом деле, согласно этой теореме сравнению

$$x^{p-1} - 1 \equiv 0 \pmod{p} \tag{14}$$

при любом простом p удовлетворяют все числа, не делящиеся на p; но эти числа по модулю p образуют $p-1$ классов, так что сравнение (14) действительно при любом простом p имеет $p-1$ решений. Как мы уже знаем, отсюда следует, что тождественно выполняется сравнение

$$x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-p+1) \pmod{p}.$$

Полагая в этом сравнении $x=0$, мы находим:

$$-1 \equiv (-1)^{p-1}(p-1)! \pmod{p};$$

если $p>2$, то $(-1)^{p-1}=1$, и следовательно,

$$(p-1)! + 1 \equiv 0 \pmod{p}; \tag{15}$$

но при $p=2$ сравнение (15) получает вид

$$2 \equiv 0 \pmod{2}$$

и, следовательно, также имеет место. Таким образом, сравнение (15) выполняется для любого простого p; это составляет содержание известной теоремы Вильсона, дающей своеобразный критерий для простых чисел. Дело в том, что ни для одного составного числа сравнение (15) не может иметь места, так как при составном p, как легко убедиться, $(p-1)!+1$ никогда не может делиться на p [1]). Правда, этот критерий Вильсона до сих пор не удалось использовать ни для каких теоретических выводов; тем не менее сам по себе он представляет значительный интерес.

Однако теорема Ферма приводит в этом круге идей и к другим, более общим и важным выводам. Умножая обе части сравнения

$$x^{p-1} \equiv 1 \pmod{p}$$

(выполняющегося согласно теореме Ферма для всех x, не

[1]) В самом деле, если p имеет такой делитель d, что $1<d<p$, то, очевидно, $(p-1)!$ делится на d; но тогда $(p-1)!+1$ не может делиться на d, а тем более на p.

делящихся на p) на x, мы приходим к сравнению

$$x^p \equiv x \pmod{p},$$

которое, конечно, также выполняется для всех упомянутых значений x; но оно тривиальным образом выполняется и для значений x, делящихся на p. Таким образом,

$$x^p \equiv x \pmod{p}$$

есть тождественное сравнение, выполняющееся для любого целого числа; иначе говоря, число $x^p - x$ при любом целом x делится на p.

Из этого, прежде всего, вытекает возможность при исследовании алгебраических сравнений по простому модулю p ограничиться сравнениями, степень которых не превосходит $p-1$. В самом деле, если $P(x)$ есть любой многочлен степени $\geqslant p$ с целыми коэффициентами, то при делении его на $x^p - x$ частное $Q(x)$ и остаток $R(x)$ также будут многочленами с целыми коэффициентами. Мы будем при этом иметь:

$$P(x) = (x^p - x)\,Q(x) + R(x),$$

и степень многочлена $R(x)$ не превосходит $p-1$. Так как $x^p - x \equiv 0 \pmod{p}$ тождественно, то всякое решение сравнения

$$P(x) \equiv 0 \pmod{p}$$

будет также удовлетворять сравнению

$$R(x) \equiv 0 \pmod{p},$$

и обратно. Таким образом, при исследовании решений каждое сравнение степени $\geqslant p$ действительно может быть заменено равносильным ему сравнением степени $< p$, причём новое сравнение находится по данному с помощью весьма элементарных алгебраических операций.

Итак, пусть

$$P(x) \equiv 0 \pmod{p} \tag{16}$$

— сравнение степени $n < p$. Последний вопрос, который мы рассмотрим, состоит в том, как узнать, будет ли число решений этого сравнения равно n или меньше n (больше n оно, как мы уже знаем, быть не может).

Прежде всего мы можем, не ограничивая общности нашей задачи, допустить, что коэффициент при x^n в многочлене $P(x)$ равен 1. В самом деле, этот коэффициент a_0 во всяком случае не делится на p; поэтому теория сравнений первой степени гарантирует нам существование такого числа a, что $a_0 a \equiv 1 \pmod{p}$. Заменяя тогда сравнение (16) равносильным ему сравнением

$$aP(x) \equiv 0 \pmod{p},$$

мы получим при x^n коэффициент $a_0 a$, который сравним с единицей по модулю p и просто может быть заменён единицей.

Итак, мы можем допустить, что у многочлена $P(x)$ коэффициент старшего члена равен 1. Поэтому, деля $x^p - x$ на $P(x)$, мы получим в частном и в остатке многочлены с целыми коэффициентами. Обозначим эти многочлены соответственно через $M(x)$ и $N(x)$, так что

$$x^p - x = P(x)\,M(x) + N(x);$$

очевидно, $M(x)$ есть многочлен степени $p - n$, а степень многочлена $N(x)$ не превосходит $n - 1$.

Допустим теперь, что сравнение (16) имеет n решений. Так как сравнение $x^p - x \equiv 0 \pmod p$ выполняется тождественно, то все эти n решений удовлетворяют и сравнению

$$N(x) = x^p - x - P(x)\,M(x) \equiv 0 \pmod p;$$

но если бы хотя один из коэффициентов многочлена $N(x)$ не делился на p, то $N(x) \equiv 0 \pmod p$ было бы сравнением степени $< n$ и не могло бы поэтому иметь n решений. Таким образом, все коэффициенты многочлена $N(x)$ должны делиться на p.

Пусть теперь, обратно, известно, что все коэффициенты многочлена $N(x)$ делятся на p, т. е. $N(x) \equiv 0 \pmod p$ тождественно; тогда тождественно

$$P(x)\,M(x) \equiv 0 \pmod p, \tag{17}$$

т. е. этому сравнению удовлетворяют все p классов по модулю p. Но любое решение сравнения (17) удовлетворяет, очевидно, по меньшей мере одному из сравнений

$$P(x) \equiv 0 \pmod p, \quad M(x) \equiv 0 \pmod p,$$

так что сумма чисел решений этих двух сравнений не может быть меньше p; но из этих сравнений второе имеет не более $p - n$ решений; отсюда и следует, что число решений сравнения (16) не может быть менее n и, значит, в точности равно n.

Таким образом, мы приходим к следующему критерию:

Теорема 8. *Для того чтобы сравнение* (16) *степени* $n < p$ *с коэффициентом* 1 *при старшем члене имело в точности* n *решений, необходимо и достаточно, чтобы все коэффициенты многочлена, получающегося в остатке при делении* $x^p - x$ *на* $P(x)$, *делились на* p.

ГЛАВА III

АЛГОРИФМ ЕВКЛИДА И ЦЕПНЫЕ ДРОБИ

§ 8. Алгорифм Евклида

Элементарная арифметика учит двум существенно различным способам нахождения наибольшего общего делителя двух чисел. Первый способ состоит в разложении данных чисел на простые множители с последующим составлением из этих множителей по известным правилам наибольшего общего делителя данных чисел. Второй способ есть так называемый способ последовательного деления: первое из данных чисел делится на второе, второе — на остаток первого деления, первый остаток на второй и т. д. Так как при этом каждый остаток меньше предыдущего и все они неотрицательны, то после конечного числа делений мы должны получить остаток, равный нулю. Последний положительный остаток в этом процессе и будет наибольшим общим делителем двух данных чисел. Этот процесс, называемый обычно «алгорифмом Евклида», замечателен своей элементарностью: для его применения нет надобности знать, как составлены данные числа из простых множителей, и в этом его существенное преимущество перед первым способом. Однако, несмотря на свою простоту и элементарность, алгорифм Евклида и по существу и исторически имеет глубокое методологическое значение. Он может быть положен в основание всей теории делимости, включая неопределённый анализ первой степени с двумя неизвестными (см. стр. 284); на нём строятся, как известно, отыскание общей меры двух величин, а вместе с тем и вся теория измерения; наконец, он служит естественным исходным пунктом теории цепных дробей — самого сильного из всех методов арифметики иррациональных чисел, имеющего также и непосредственное практическое значение.

Мы поэтому со всею тщательностью рассмотрим теперь этот алгорифм и его арифметические приложения.

Пусть даны два целых числа a и b, из которых второе положительно. Будем делить a на b и обозначим соответственно через a_1 и r_1 частное и остаток этого деления, так что

$$a = ba_1 + r_1 \qquad (0 \leqslant r_1 < b). \tag{1}$$

Если $r_1 > 0$, то будем делить b на r_1 и обозначим соответственно через a_2 и r_2 частное и остаток этого деления, так что

$$b = r_1 a_2 + r_2 \qquad (0 \leqslant r_2 < r_1); \tag{2}$$

если r_2 всё ещё не нуль, делим r_1 на r_2 и получаем аналогичным образом:

$$r_1 = r_2 a_3 + r_3 \qquad (0 \leqslant r_3 < r_2).$$

Так как $b > r_1 > r_2 > r_3 > \ldots \geqslant 0$, то начатый таким образом процесс после конечного числа шагов должен оборваться, т. е. рано или поздно мы должны прийти к остатку, равному нулю. Пусть впервые $r_{n+1} = 0$, так что

$$r_{n-1} = r_n a_{n+1}.$$

Тогда r_n есть наибольший общий делитель чисел a и b. Чтобы в этом убедиться, покажем, прежде всего, что a и b делятся на r_n. В силу последнего написанного равенства r_{n-1} делится на r_n; но тогда предпоследнее (не выписанное нами) равенство

$$r_{n-2} = r_{n-1} a_n + r_n \tag{3}$$

показывает, что и r_{n-2} делится на r_n. Продвигаясь далее (в обратном порядке) в цепи построенных нами равенств, мы убедимся, что на r_n делятся и r_{n-3}, r_{n-4}, ... , r_1, а в конечном счёте в силу равенств (2) и (1) — числа a и b. Теперь покажем, что всякий общий делитель d чисел a и b будет и делителем числа r_n (этим, очевидно, и будет установлено, что r_n есть наибольший общий делитель чисел a и b). Для этого нам снова придётся пройти цепь построенных нами равенств, но на этот раз — сверху вниз. Равенство (1), которое может быть записано в виде

$$r_1 = a - ba_1,$$

показывает нам, что всякий общий делитель d чисел a и b есть вместе с тем делитель числа r_1; но в таком случае равенство (2) аналогичным образом показывает, что и r_2 делится на d, и т. д. В конечном счёте мы придём к равенству (3); так как при этом делимость чисел r_{n-2} и r_{n-1} на d уже будет установлена, то это равенство и покажет нам, что r_n делится на d.

Этот способ отыскания наибольшего общего делителя двух чисел с помощью алгорифма Евклида в большинстве случаев оказывается самым коротким и потому практически наиболее выгодным. С теоретической стороны интересно отметить, что в только что проведённом рассуждении мы попутно доказали теорему о том, что всякий общий делитель двух чисел есть делитель их наибольшего общего делителя.

Теперь мы покажем, как на основе алгорифма Евклида может быть построена вся теория делимости. Равенство (1) показывает

нам, что число r_1 может быть представлено как «линейная комбинация» чисел a и b, т. е. как выражение вида $ax+by$, где x и y — целые числа ($x=1$, $y=-a_1$); но в таком случае из равенства (2) следует, что $r_2=b-r_1a_2$ также может быть представлено в виде линейной комбинации чисел a и b:

$$r_2=b-(ax+by)\,a_2=a\,(-a_2x)+b\,(1-a_2y).$$

Спускаясь снова в нашей цепи равенств, мы таким образом постепенно убеждаемся в возможности выразить в виде $ax+by$ числа r_3, r_4, ...; наконец, равенство (3), в котором числа r_{n-2} и r_{n-1} в этом виде уже выражены, очевидно, позволит нам представить и r_n как линейную комбинацию чисел a и b. Мы приходим, таким образом, к хорошо знакомой нам из главы I теореме: *наибольший общий делитель двух чисел всегда может быть представлен в виде линейной комбинации этих чисел.* В частном случае, когда числа a и b взаимно просты, это даёт теорему 1 главы I (см. стр. 258).

Мы получили, таким образом, уже третье доказательство этой теоремы и притом такое, которое одновременно даёт кратчайший путь к отысканию искомых чисел x и y. Когда мы ознакомимся с элементами теории цепных дробей, мы увидим ещё более удобное расположение операций, ведущих к отысканию этих чисел.

Из теоремы 1, как мы видели в главе I, немедленно вытекает теорема 2, на которой базируется доказательство фундаментальной теоремы о единственности разложения чисел на простые множители, а значит, и вся теория делимости. Вместе с тем эта же теорема 1 служит основанием и всей теории уравнений первой степени с двумя неизвестными.

Но значение алгорифма Евклида выходит далеко за пределы арифметики натуральных чисел. Не говоря уже о том, что этот метод позволяет построить теорию делимости для целых чисел ряда алгебраических областей, алгорифм Евклида служит наилучшей базой для обоснования теории делимости многочленов с одной переменной в алгебре. Этот вопрос, по своей элементарности непосредственно примыкающий к школьному курсу алгебры, нам необходимо рассмотреть здесь подробно; при этом мы сможем только во многих случаях вести изложение значительно короче, ссылаясь на почти полную аналогию с вышеприведёнными рассуждениями.

Объектом наших действий будут теперь не числа, а многочлены вида

$$P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

где коэффициенты a_0, a_1, ..., a_n — рациональные числа.

Мы называем многочлен $P(x)$ многочленом степени n, если $a_0\neq 0$. Если $A(x)$ и $B(x)$ — два таких многочлена, причём $B(x)$ не есть постоянное число (т. е. многочлен, все коэффициенты которого, кроме свободного члена, равны нулю), то элементарный про-

цесс деления, подробно излагаемый в школьных учебниках алгебры, показывает, что всегда существует два таких многочлена $Q(x)$ и $R(x)$, что тождественно

$$A(x) = Q(x)\,B(x) + R(x), \tag{4}$$

причём степень многочлена $R(x)$ (остатка) меньше степени многочлена $B(x)$ (делителя). Многочлены $Q(x)$ (частное) и $R(x)$ (остаток) при этом определены однозначно. В самом деле, если наряду с (4) мы имеем другое соотношение того же вида, например

$$A(x) = Q'(x)\,B(x) + R'(x),$$

где степень $R'(x)$ также ниже степени $B(x)$, то тождественно

$$R(x) + Q(x)\,B(x) = R'(x) + Q'(x)\,B(x),$$

откуда

$$[Q(x) - Q'(x)]\,B(x) = R'(x) - R(x).$$

Степень многочлена, стоящего в правой части этого равенства, ниже степени $B(x)$; для левой части это, очевидно, возможно лишь при условии, что тождественно $Q'(x) = Q(x)$, вследствие чего и $R'(x) = R(x)$. Коэффициенты многочленов $Q(x)$ и $R(x)$ получаются из коэффициентов $A(x)$ и $B(x)$ рациональными операциями и будут поэтому также рациональными числами.

В дальнейшем мы вообще будем понимать равенство двух многочленов как попарное равенство всех коэффициентов при одинаковых степенях x; в частности, $P(x) = 0$ означает, что все коэффициенты многочлена $P(x)$ равны нулю.

Если в соотношении (4) $R(x) = 0$, т. е. если $A(x)$ может быть представлено в виде $B(x)Q(x)$, то говорят, что многочлен $A(x)$ *делится* (без остатка) на многочлен $B(x)$. Таким образом, делимость в нашей области определяется в точности так же, как в области целых чисел. Если r — любое рациональное число, отличное от нуля, а $P(x)$ — многочлен с рациональными коэффициентами, то таким же будет и многочлен $\frac{P(x)}{r}$. Соотношение

$$A(x) = r \cdot \frac{A(x)}{r}$$

показывает, что любой многочлен $A(x)$ делится на любое рациональное число r (кроме нуля) и на любой многочлен вида $\frac{A(x)}{r}$. Таким образом, в нашей теории делимости любое рациональное число играет роль единицы. Естественно поэтому называть *взаимно простыми* два многочлена, не имеющих других общих делителей, кроме рациональных чисел. Далее, мы называем *абсолютно простым* (или *неприводимым*) многочлен $P(x)$, не имеющий других делителей,

кроме рациональных чисел r и многочленов вида $\frac{P(x)}{r}$. При этом только сами рациональные числа к простым многочленам не причисляются, подобно тому как в теории делимости целых чисел единицу не причисляют к простым числам.

Соотношение (4), совершенно аналогичное соотношению между делимым, делителем, частным и остатком в теории целых чисел, может и здесь стать исходной точкой для построения алгорифма Евклида и тем самым как бы в зародыше уже содержит в себе всю теорию делимости. В случае целых чисел решающим моментом было то, что при всяком делении остаток меньше делителя; именно на этом основывалась конечная длительность алгорифма. В случае же многочленов у нас степень остатка всегда меньше степени делителя. Но так как натуральное число, что бы оно ни означало, при непрестанном понижении через конечное число шагов должно дойти до нуля, то и здесь конечность процесса нам гарантирована.

Формальная сторона алгорифма протекает в столь полной аналогии со случаем целых чисел, что нам нет надобности воспроизводить её здесь в деталях. Мы делим $A(x)$ на $B(x)$, затем $B(x)$ на первый остаток, затем первый остаток на второй и т. д. Покуда остаток не есть число (т. е. имеет положительную степень), степень следующего остатка будет ниже степени данного; если же мы придём к остатку степени 0 (т. е. к рациональному числу), то следующий остаток равен нулю. Таким образом, во всех случаях рано или поздно остаток обратится в нуль. Обозначая через $R_n(x)$ последний остаток, отличный от нуля (он может, в частности, оказаться и числом), мы будем иметь, как и в случае целых чисел, соотношения

$$R_{n-2}(x) = Q_n(x)\,R_{n-1}(x) + R_n(x),$$
$$R_{n-1}(x) = Q_{n+1}(x)\,R_n(x).$$

Первое из них показывает, если учесть второе, что и $R_{n-2}(x)$ делится на $R_n(x)$; восходя же в цепи полученных равенств всё выше и выше, мы в конечном счёте убедимся, как в случае целых чисел, что и оба исходных многочлена делятся на $R_n(x)$. Итак, $R_n(x)$ есть общий делитель двух данных многочленов. Но далее, проходя ряд полученных равенств в нисходящем порядке, мы так же, как и в случае целых чисел, убеждаемся, что всякий общий делитель $D(x)$ многочленов $A(x)$ и $B(x)$ есть вместе с тем делитель и многочлена $R_n(x)$. Таким образом, $R_n(x)$ есть такой общий делитель многочленов $A(x)$ и $B(x)$, который делится на всякий другой их общий делитель. Естественно поэтому называть $R_n(x)$ *наибольшим* общим делителем многочленов $A(x)$ и $B(x)$; это тем более естественно, что многочлены мы не можем сравнивать по величине, и поэтому обычное в теории целых чисел определение наибольшего общего делителя не может быть перенесено в область

многочленов. Впрочем, и здесь наибольший общий делитель обладает весьма простым максимальным свойством, которое мы должны теперь установить, тем более, что именно этим путём мы сможем разобраться в вопросе о единственности наибольшего общего делителя; этот вопрос, который для целых чисел, очевидно, решается автоматически, здесь требует, напротив, особого рассмотрения.

Прежде всего ясно, что наряду с наибольшим общим делителем $D(x)$ многочленов $A(x)$ и $B(x)$ тому же определению будет удовлетворять и любой многочлен вида $rD(x)$, где r — любое отличное от нуля рациональное число. Таким образом, любые два многочлена имеют бесконечное множество наибольших общих делителей, отличающихся друг от друга постоянными множителями; это не должно казаться нам странным, так как мы уже знаем, что в нашей теории все рациональные числа играют роль единицы. Отличие между двумя такими наибольшими общими делителями в такой мере тривиально, что мы можем считать их лишь несущественно различными. Легко теперь убедиться, что *всякий общий делитель* $D'(x)$ *многочленов* $A(x)$ *и* $B(x)$, *существенно* (т. е. не только постоянным множителем) *отличный от* $D(x)$, *должен иметь степень, низшую, чем* $D(x)$. В самом деле, если $D(x)$ — число, то $D'(x)$ как делитель $D(x)$ также есть число и, значит, лишь несущественно отличается от $D(x)$; если же степень $D(x)$ положительна, то частное от деления $D(x)$ на $D'(x)$ в силу их существенного различия должно иметь положительную степень, и следовательно, степень $D'(x)$ ниже степени $D(x)$, что и надо было установить. Можно, таким образом, сказать, что *наибольший общий делитель двух многочленов определён однозначно с точностью до произвольного постоянного рационального множителя.*

Алгорифм Евклида, позволяющий, таким образом, найти наибольший общий делитель двух многочленов, вместе с тем и здесь, как в теории целых чисел, может служить базой для построения всей теории делимости. Прежде всего мы можем здесь в точной аналогии с тем, как мы это сделали выше для целых чисел, показать, что наибольший общий делитель двух многочленов может быть представлен в виде линейной комбинации этих многочленов; коэффициентами этой комбинации служат, разумеется, также некоторые многочлены с рациональными коэффициентами. Из этого, в частности, вытекает предложение, аналогичное теореме 1 главы I: *если многочлены* $A(x)$ *и* $B(x)$ *взаимно просты, то существуют такие многочлены* $X(x)$ *и* $Y(x)$, *что*

$$A(x)X(x) + B(x)Y(x) = 1.$$

Это, прежде всего, показывает, что основная задача неопределённого анализа первой степени с двумя неизвестными для многочленов с рациональными коэффициентами решается в том же смысле, как и для целых чисел. Далее, следуя в точности по пути, изложен-

ному в главе I, мы легко приходим к теореме, аналогичной теореме 2; отсюда же в точности так же, как там, может быть установлена однозначная (с точностью до постоянных множителей) разложимость многочленов на простые множители, служащая фундаментом всей теории делимости.

Упомянем, наконец, что теорема Евклида о существовании бесконечного множества простых чисел вместе с её доказательством легко переносится в нашу новую область. Впрочем, существование бесконечного множества абсолютно простых многочленов ещё проще вытекает из того, что все двучлены первой степени, как читатель легко докажет самостоятельно, являются абсолютно простыми многочленами.

§ 9. Элементарная теория цепных дробей

Мы возвращаемся в область целых чисел. Выпишем снова цепь равенств, с помощью которых мы находим наибольший общий делитель чисел a и b:

$$\begin{aligned} a &= ba_1 + r_1, \\ b &= r_1a_2 + r_2, \\ r_1 &= r_2a_3 + r_3, \\ &\dots\dots\dots \\ r_{n-2} &= r_{n-1}a_n + r_n, \\ r_{n-1} &= r_na_{n+1}, \end{aligned}$$

где

$$b > r_1 > r_2 > \dots > r_n > 0. \tag{5}$$

Мы можем переписать эту цепь в виде равносильной системы равенств

$$\begin{aligned} \frac{a}{b} &= a_1 + \frac{r_1}{b}, \\ \frac{b}{r_1} &= a_2 + \frac{r_2}{r_1}, \\ \frac{r_1}{r_2} &= a_3 + \frac{r_3}{r_2}, \\ &\dots\dots\dots \\ \frac{r_{n-2}}{r_{n-1}} &= a_n + \frac{r_n}{r_{n-1}}, \\ \frac{r_{n-1}}{r_n} &= a_{n+1}. \end{aligned}$$

В этом виде каждое из наших равенств описывает простую арифметическую операцию: исключение целой части из неправильной

дроби, т. е. представление неправильной дроби в виде суммы целого числа и некоторой правильной дроби. Действительно, в силу неравенств (5) левые части всех этих равенств представляют собой неправильные дроби, а вторые слагаемые правых частей — дроби правильные. Отметим ещё, что левая часть каждого равенства (начиная со второго) есть обратная величина второго слагаемого правой части предыдущего равенства.

Поставим себе теперь задачу выразить отношение $\frac{a}{b}$ через одни только числа $a_1, a_2, \ldots, a_n$. Сделать это с помощью нашей цепи равенств очень легко. Первое равенство даёт:

$$\frac{a}{b} = a_1 + \cfrac{1}{\cfrac{b}{r_1}};$$

подставляя сюда вместо $\frac{b}{r_1}$ его выражение из второго равенства, мы находим:

$$\frac{a}{b} = a_1 + \cfrac{1}{a_2 + \cfrac{r_2}{r_1}} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cfrac{r_1}{r_2}}};$$

вставляя сюда вместо $\frac{r_1}{r_2}$ его выражение из третьего равенства, получаем:

$$\frac{a}{b} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{r_3}{r_2}}} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cfrac{r_2}{r_3}}}}$$

и т. д. В конце концов, мы находим:

$$\begin{aligned} \frac{a}{b} &= a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{\cfrac{r_{n-1}}{r_n}}}} = \\ &= a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_{n+1}}}}. \end{aligned} \tag{6}$$

Выражение такого вида, как правая часть этого равенства, называется *цепной* или *непрерывной дробью*. Здесь a_1 — целое число

(которое может быть и отрицательным и нулём), в то время как a_2, a_3, ..., a_{n+1} — натуральные числа.

Мы видим, таким образом, что алгорифм Евклида получает для нас новое и очень важное значение: он доказывает возможность представления любой простой дроби в виде цепной дроби и вместе с тем позволяет фактически получить это представление.

Элементарная арифметика учит нас представлять рациональные числа в нескольких различных видах: в виде простых или обыкновенных дробей; в виде десятичных (и вообще систематических, т. е. отнесённых к определённой системе счисления) дробей, конечных или бесконечных периодических; наконец, в процентном исчислении. Наряду с этими различными представлениями, каждое из которых имеет свои преимущества, представление чисел в виде непрерывных дробей также играет важнейшую роль как в развитии теории, так и для непосредственных практических приложений. Поэтому учение о цепных дробях получило очень широкое развитие, продолжающееся и до настоящего времени.

В целях сокращения записи цепную дробь, стоящую в правой части равенства (6), обычно символически записывают в виде

$$[a_1;\ a_2,\ a_3,\ \ldots,\ a_{n+1}];$$

точка с запятой после a_1 имеет целью подчеркнуть роль a_1 как «целой части» изображаемого данной цепной дробью числа. Числа a_1, a_2, ..., a_{n+1} называются *элементами* данной цепной дроби; иногда их называют *неполными частными* — название, напоминающее их происхождение из алгорифма Евклида.

Прежде всего встаёт, разумеется, вопрос о единственности представления данного рационального числа цепною дробью. Могут ли две различные цепные дроби изображать одно и то же число, т. е. попросту быть равны друг другу? Что это, вообще говоря, возможно, показывает уже тривиальный по своей простоте пример:

$$\frac{1}{2}=\frac{1}{1+\frac{1}{1}},$$

или в символической форме

$$[0;\ 2]=[0;\ 1,\ 1].$$

Вообще, если $a_{n+1}>1$, то

$$a_{n+1}=(a_{n+1}-1)+\frac{1}{1},$$

а поэтому

$$[a_1;\ a_2,\ \ldots,\ a_{n+1}]=[a_1;\ a_2,\ \ldots,\ a_{n+1}-1,\ 1].$$

Однако эта двузначность имеет столь же тривиальный характер, как в теории десятичных дробей, например двузначность представления

$$1 = 0{,}999\ldots;$$

и как там мы уничтожаем эту двузначность простым соглашением не пользоваться разложениями, оканчивающимися бесконечным рядом девяток, так и здесь мы можем условиться исключить из рассмотрения все цепные дроби, у которых $a_{n+1} = 1$. Это всегда возможно, так как дробь

$$[a_1;\ a_2,\ \ldots,\ a_{n-1},\ a_n,\ 1]$$

всегда равна дроби

$$[a_1;\ a_2,\ \ldots,\ a_{n-1},\ a_n + 1],$$

у которой последний элемент больше единицы.

Покажем теперь, что, приняв только что упомянутое соглашение, мы тем самым обеспечиваем единственность представления всякого рационального числа в виде цепной дроби. Пусть

$$[a_0;\ a_1,\ a_2,\ \ldots,\ a_r] = [b_0;\ b_1,\ b_2,\ \ldots,\ b_s],$$

причём $a_r > 1$ и $b_s > 1$; требуется доказать, что $r = s$, $a_0 = b_0$, $a_1 = b_1$, $\ldots$, $a_r = b_r$.

Из

$$a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_r}} = b_0 + \cfrac{1}{b_1 + \ddots + \cfrac{1}{b_s}}$$

следует, что целые части левой и правой дробей должны быть одинаковы; но второе слагаемое левой дроби есть правильная дробь, так как единице оно может равняться лишь при $r = 1$, $a_1 = 1$ — случай, исключённый нашим требованием $a_r > 1$. Поэтому целая часть левой дроби есть a_0; по такой же причине целая часть правой дроби есть b_0 и, следовательно, $a_0 = b_0$. Но если так, то наше равенство даёт:

$$a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_r}} = b_1 + \cfrac{1}{b_2 + \ddots + \cfrac{1}{b_s}};$$

тем же путём, каким мы установили $a_0 = b_0$, мы отсюда находим, что $a_1 = b_1$. Продолжая этот процесс достаточное число раз, мы, очевидно, постепенно установим всё, что требовалось доказать. Таким образом, единственность разложения числа в цепную дробь мы можем считать установленной.

Теперь мы введём основное для всей теории понятие подходящей дроби. Пусть мы имеем произвольную цепную дробь

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}} = [a_0;\ a_1, a_2,\ \ldots,\ a_n].$$

Рассмотрим тогда ряд выражений $[a_0]$, $[a_0;\ a_1]$, $[a_0;\ a_1,\ a_2]$, ..., $[a_0;\ a_1,\ a_2,\ \ldots,\ a_{n-1}]$, $[a_0;\ a_1,\ a_2,\ \ldots,\ a_n]$, последнее из которых есть данная цепная дробь, а предыдущие получаются её «обрыванием» на том или другом неполном частном a_k. Каждое из этих выражений можно вычислить, т. е. свернуть в простую дробь:

$$[a_0] = a_0 = \frac{a_0}{1},$$

$$[a_0;\ a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1},$$

$$[a_0;\ a_1,\ a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \frac{(a_0 a_1 + 1)\, a_2 + a_0}{a_1 a_2 + 1},$$

и т. д. Получающийся при этом ряд простых дробей мы и называем *подходящими дробями* данной цепной дроби (или представляемого ею числа $\frac{a}{b}$); мы будем последовательно обозначать эти дроби через $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n}$, так что, в частности,

$$\left.\begin{aligned} &p_0 = a_0,\ p_1 = a_0 a_1 + 1,\ p_2 = (a_0 a_1 + 1)\, a_2 + a_0, \\ &q_0 = 1,\ q_1 = a_1,\ q_2 = a_1 a_2 + 1. \end{aligned}\right\} \qquad (7)$$

Очевидно, что

$$\frac{p_n}{q_n} = \frac{a}{b}.$$

Далее, соотношения (7) показывают, что

$$p_2 = p_1 a_2 + p_0,$$
$$q_2 = q_1 a_2 + q_0.$$

Чрезвычайно важно, что этот «закон образования» числителей и знаменателей подходящих дробей является всеобщим: для любого k $(2 \leqslant k \leqslant n)$ мы имеем:

$$\left.\begin{aligned} p_k &= p_{k-1} a_k + p_{k-2}, \\ q_k &= q_{k-1} a_k + q_{k-2}. \end{aligned}\right\} \qquad (8)$$

Так как для $k=2$ эти соотношения уже установлены, то нам остаётся только показать, что если они верны для некоторого числа $k<n$, то они остаются верными и для числа $k+1$. Но при $k<n$

$$\frac{p_k}{q_k}=a_0+\cfrac{1}{a_1+\cfrac{1}{\ddots+\cfrac{1}{a_k}}},$$

$$\frac{p_{k+1}}{q_{k+1}}=a_0+\cfrac{1}{a_1+\cfrac{1}{\ddots+\cfrac{1}{a_k+\cfrac{1}{a_{k+1}}}}};$$

значит, для получения дроби $\frac{p_{k+1}}{q_{k+1}}$ надо только в выражении дроби $\frac{p_k}{q_k}$ заменить a_k на $a_k+\frac{1}{a_{k+1}}$ всюду, где оно встречается. Но в силу (8) мы имеем:

$$\frac{p_k}{q_k}=\frac{p_{k-1}a_k+p_{k-2}}{q_{k-1}a_k+q_{k-2}}, \tag{9}$$

причём p_{k-1}, p_{k-2}, q_{k-1}, q_{k-2}, очевидно, зависят только от a_0, a_1, ..., a_{k-1}, но не зависят от a_k; поэтому

$$\frac{p_{k+1}}{q_{k+1}}=\frac{p_{k-1}\left(a_k+\frac{1}{a_{k+1}}\right)+p_{k-2}}{q_{k-1}\left(a_k+\frac{1}{a_{k+1}}\right)+q_{k-2}}=$$

$$=\frac{(p_{k-1}a_k+p_{k-2})a_{k+1}+p_{k-1}}{(q_{k-1}a_k+q_{k-2})a_{k+1}+q_{k-1}}=\frac{p_ka_{k+1}+p_{k-1}}{q_ka_{k+1}+q_{k-1}},$$

т. е. p_{k+1} и q_{k+1} действительно выражаются по формулам (8) с заменою k на $k+1$.

Примечание. Мы скоро убедимся, что если p_k и q_k построены согласно рекуррентным формулам (8), то дроби (9) все несократимы. Прежде чем это установлено, мы просто условливаемся принимать за числители и знаменатели подходящих дробей именно числа p_k и q_k, рекуррентно получаемые по формулам (8), не заботясь при этом о несократимости дробей (9).

Дробь $\frac{p_k}{q_k}$ называется *подходящей дробью порядка* k; очевидно, эта дробь является функцией элементов a_0, a_1, a_2, ..., a_k. Соотношение (9), в котором, как уже было подчёркнуто, p_{k-1}, q_{k-1}, p_{k-2}, q_{k-2} от a_k не зависят, показывает, что при фиксированных (т. е. получивших определённые числовые значения) a_0, a_1, ..., a_{k-1} дробь $\frac{p_k}{q_k}$ становится простой дробно-линейной функцией

от a_k. В этом и состоит главное значение рекуррентных формул (8), на которых строится вся теория цепных дробей.

Теперь мы установим ряд важнейших свойств подходящих дробей. Введём обозначение

$$q_k p_{k+1} - p_k q_{k+1} = \Delta_k \quad (k = 0,\ 1,\ \ldots,\ n-1).$$

В силу рекуррентных формул (8)

$$\Delta_k = q_k(p_k a_{k+1} + p_{k-1}) - p_k(q_k a_{k+1} + q_{k-1}) =$$
$$= -(q_{k-1}p_k - p_{k-1}q_k) = -\Delta_{k-1};$$

таким образом, все величины Δ_k имеют одно и то же абсолютное значение, а знаки их чередуются; замечая же, что в силу (7)

$$\Delta_0 = q_0 p_1 - p_0 q_1 = 1,$$

мы приходим к следующему важному предложению:

Теорема 1. $\Delta_k = (-1)^k$ $(0 \leqslant k < n)$.

Отсюда, прежде всего, вытекает несократимость всех подходящих дробей. В самом деле, если бы p_k и q_k делились на одно и то же число $d > 1$, то, очевидно, на него делилось бы и Δ_k, что невозможно в силу теоремы 1.

Далее, если наша исходная дробь $\frac{a}{b}$ несократима, то $a = p_n$, $b = q_n$, и мы имеем:

$$\Delta_{n-1} = q_{n-1}a - p_{n-1}b = (-1)^{n-1}.$$

Таким образом (уже в четвёртый раз), мы доказали теорему о том, что если числа a и b взаимно просты, то уравнение

$$ax + by = 1$$

имеет решения в целых x, y; на этот раз мы вместе с тем получили и такой метод отыскания этих решений, который на практике в большинстве случаев оказывается кратчайшим. Мы видим, что для этого надо разложить $\frac{a}{b}$ в цепную дробь, и если $a = p_n$, $b = q_n$, то положить $x = (-1)^{n-1}q_{n-1}$, $y = (-1)^n p_{n-1}$.

Пример. Пусть $a = 52$, $b = 23$; мы находим:

$$\frac{52}{23} = 2 + \frac{6}{23} = 2 + \cfrac{1}{3 + \cfrac{5}{6}} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}} = \frac{p_3}{q_3};$$

$$\frac{p_2}{q_2} = 2 + \cfrac{1}{3 + \cfrac{1}{1}} = \frac{9}{4};$$

$$x = 4, \quad y = -9, \quad ax + by = 1.$$

С другой стороны, теорема 1 даёт возможность сделать весьма полные выводы о взаимном расположении подходящих дробей. В самом деле, из $\Delta_k = (-1)^k$ следует:

$$\frac{\Delta_k}{q_k q_{k+1}} = \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k+1}},$$

т. е. для чётных k мы имеем: $\frac{p_{k+1}}{q_{k+1}} > \frac{p_k}{q_k}$, а для нечётных: $\frac{p_{k+1}}{q_{k+1}} < \frac{p_k}{q_k}$. Начнём с пары $\frac{p_0}{q_0}$, $\frac{p_1}{q_1}$ (рис. 1). Очевидно, $\frac{p_1}{q_1} > \frac{p_0}{q_0}$; далее, мы знаем, что $\frac{p_2}{q_2} < \frac{p_1}{q_1}$; но так как расстояние от $\frac{p_1}{q_1}$ до $\frac{p_2}{q_2}$, равное $\left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right| = \frac{1}{q_1 q_2}$, меньше, чем расстояние $\left|\frac{p_1}{q_1} - \frac{p_0}{q_0}\right| = \frac{1}{q_0 q_1}$ от $\frac{p_1}{q_1}$ до $\frac{p_0}{q_0}$, то $\frac{p_2}{q_2}$ лежит между $\frac{p_0}{q_0}$ и $\frac{p_1}{q_1}$, как и отмечено на рис. 1.

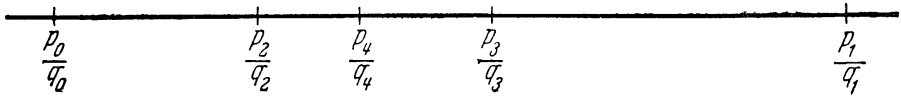


Рис. 1.

Переходя теперь к отысканию положения дроби $\frac{p_3}{q_3}$, мы, прежде всего, замечаем, что $\frac{p_3}{q_3} > \frac{p_2}{q_2}$; но так как, с другой стороны,

$$\left|\frac{p_3}{q_3} - \frac{p_2}{q_2}\right| = \frac{1}{q_2 q_3} < \frac{1}{q_1 q_2} = \left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right|,$$

то $\frac{p_3}{q_3}$ лежит к $\frac{p_2}{q_2}$ ближе, чем $\frac{p_1}{q_1}$, т. е. $\frac{p_3}{q_3}$ лежит между $\frac{p_2}{q_2}$ и $\frac{p_1}{q_1}$, как и отмечено на рис. 1. Очевидно, что мы можем продолжать это рассуждение вплоть до $\frac{p_n}{q_n} = \frac{a}{b}$; выводом из него, очевидно, является следующее предложение:

Теорема 2. *Все подходящие дроби чётного порядка меньше* $\frac{a}{b}$, *и величина их возрастает с ростом порядка; все подходящие дроби нечётного порядка больше* $\frac{a}{b}$, *и величина их убывает с ростом порядка.*

Из этой теоремы, в частности, следует, что число $\frac{a}{b}$ заключено между двумя любыми своими последовательными подходящими дробями $\frac{p_k}{q_k}$ и $\frac{p_{k+1}}{q_{k+1}}$, и следовательно, расстояние между $\frac{a}{b}$ и каждой из этих двух дробей меньше расстояния между самими этими

дробями, которое равно $\frac{1}{q_k q_{k+1}}$. Мы приходим, таким образом, к предложению, играющему основную роль во всех вопросах приближённого представления чисел.

Теорема 3.

$$\left|\frac{a}{b} - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}.$$

Теория цепных дробей исторически возникла из потребности приближённо представить дробь, числитель и знаменатель которой очень велики, другою дробью, у которой они значительно меньше. Творец теории цепных дробей Христиан Гюйгенс при построении модели солнечной системы с помощью набора зубчатых колёс встретился со своеобразным затруднением: для того чтобы отношение времён оборота двух зацепляющихся зубчатых колёс равнялось отношению времён оборота вокруг солнца двух изображаемых этими колёсами планет, надо, чтобы в том же отношении стояли и числа зубцов этих двух колёс. Однако отношение это выражается столь большими числами, что технически невозможно изготовить колёса с такими «астрономическими» числами зубцов. Поэтому возникает необходимость ограничиться приближённой моделью, выбирая числа зубцов технически осуществимыми и вместе с тем так, чтобы отношение этих чисел было, по возможности, близко к заданному отношению очень больших чисел. Здесь и приходят на помощь цепные дроби. Пусть a и b — те большие числа, отношение которых мы хотим в порядке приближения заменить отношением меньших чисел c и d; для определённости допустим, что по техническим или иным условиям число d не должно превышать 100. Тогда мы представляем отношение $\frac{a}{b}$ в виде цепной дроби и вычисляем последовательные подходящие дроби. Пусть при этом оказалось, что $q_k \leqslant 100$, но уже $q_{k+1} > 100$. Тогда мы полагаем $c = p_k$, $d = q_k$, и теорема 3 позволяет нам просто и удобно оценить ту погрешность, которую мы сделаем, заменив отношение $\frac{a}{b}$ отношением $\frac{c}{d}$.

Пример. $a = 1355$, $b = 946$. Мы находим:

$$\frac{a}{b} = [1;\ 2,\ 3,\ 5,\ 8,\ 3],$$

$$\frac{p_3}{q_3} = \frac{53}{37}, \quad \frac{p_4}{q_4} = \frac{434}{303},$$

$$\left|\frac{a}{b} - \frac{p_3}{q_3}\right| = \left|\frac{1355}{946} - \frac{53}{37}\right| < \frac{1}{q_3 q_4} = \frac{1}{11211} < 0{,}0001.$$

Если бы мы хотели получить решение нашей задачи с помощью десятичных, а не цепных дробей, то для достижения такой точности нам пришлось бы взять дробь по меньшей мере с четырьмя

знаками после запятой, т. е. дробь со знаменателем 10 000; но это не имело бы никакого смысла, так как сама представляемая дробь имеет знаменатель 946. Поэтому для задач подобного рода аппарат цепных дробей не только имеет преимущество перед десятичными дробями, но во многих случаях (подобно приведённому нами примеру) позволяет найти решение задачи там, где десятичные дроби ничего не позволяют сделать. Дело в том, что в случае цепных дробей в качестве знаменателей можно выбирать любые числа, а не только степени десяти, и это даёт значительно больший простор для выбора. Конечно, не надо при этом терять из виду, что в других отношениях десятичные (и вообще систематические) дроби имеют существенные преимущества перед цепными. Так, всем известно, с какою лёгкостью производятся арифметические действия над десятичными дробями, между тем как никому ещё не удалось найти правила сложения двух цепных дробей. Правильная позиция здесь, как всегда, состоит не в том, чтобы спорить о сравнительных преимуществах этих двух замечательных аппаратов, а в том, чтобы полностью овладеть обоими и пользоваться каждым в надлежащий момент и в надлежащем месте.

ГЛАВА IV

ПРЕДСТАВЛЕНИЕ ЧИСЕЛ СИСТЕМАТИЧЕСКИМИ И ЦЕПНЫМИ ДРОБЯМИ

§ 10. Введение

Оба аппарата — систематические (в частности, десятичные) и цепные дроби — полностью осуществляют своё назначение лишь тогда, когда мы охватываем ими всю совокупность действительных (в том числе и иррациональных) чисел. В самом деле, для рациональных чисел простые (обыкновенные) дроби являются таким формальным аппаратом, который в большинстве встречающихся задач оказывается вполне удовлетворительным и лишь в отдельных случаях заставляет искать иных формальных приёмов исследования. Для иррациональных же чисел мы никакого аналогичного аппарата не имеем; для них весь арсенал формальных орудий исследования и оперирования впервые создаётся систематическими или цепными дробями.

Как мы уже говорили, систематические дроби имеют своим главным преимуществом ту замечательную простоту, с какою они подвергаются основным арифметическим операциям. Но если мы ставим себе задачу исследовать арифметическую природу какого-либо числа, всё равно — рационального или иррационального, — то представлять его для этого в виде систематической (например, десятичной) дроби было бы нецелесообразно: чередование цифр в этой дроби характеризует собою не абсолютную природу данного числа, которая нас интересует, а лишь его взаимоотношение с выбранной системой счисления; достаточно вспомнить, что одно и то же число может изображаться в одной системе конечной, а в другой бесконечной систематической дробью. Напротив, алгорифм цепных дробей, не зависящий ни от какой системы счисления, даёт такое представление чисел, которое обусловлено исключительно собственной их арифметической природой и потому наилучшим образом приспособлено к исследованию этой природы.

Наша средняя школа, обучая детей действиям над десятичными дробями, почти не касается теоретических основ этого аппарата.

Это объясняется тем, что десятичные дроби изучаются в пятом классе, когда усвоение строгой теории систематических дробей потребовало бы навыков формального мышления, значительно превосходящих возрастные возможности учащихся. Поэтому и учебники арифметики для средней школы либо вовсе не касаются этой теории, либо лишь на примерах, без общих рассуждений, устанавливают её основные положения. А между тем учитель не может, конечно, уверенно вести преподавание учения о десятичных дробях, если ему самому теоретическая база этого учения не ясна во всех своих частях.

Что касается цепных дробей, то в данный момент средняя школа совсем не включает их в свои программы. Однако это учение, будучи одним из самых живых и действенных арифметических завоеваний классической эпохи и притом таким, которое и до сих пор остаётся важнейшим вспомогательным орудием математического научного творчества, бесспорно должно стать достоянием каждого культурного математика.

§ 11. Систематические дроби

Мы возьмём за основание системы счисления произвольное целое число $k > 1$; мы будем, следовательно, говорить о представлении чисел k-ичными дробями. Как известно, в приложениях обычно выбирают $k = 10$; но для построения теории совершенно безразлично, какое число выбрано основанием системы счисления, и потому здесь у нас нет никаких причин фиксировать этот выбор. В качестве представляемого числа может фигурировать любое действительное число α. Только для того, чтобы технически немного упростить расчёты и их запись, мы будем всегда предполагать, что $0 \leqslant \alpha < 1$. Таким образом, целые части наших k-ичных дробей мы всегда будем предполагать равными нулю; совершенно очевидно, что это не внесёт в наши рассуждения никаких существенных ограничений и что добавление, в случае надобности, к нашим дробям тех или иных целых чисел не вызовет никаких добавочных затруднений.

Определение 1. *Числа* $0, 1, 2, \ldots, k-1$ *называются цифрами.*

Определение 2. *Пусть дана бесконечная последовательность цифр*

$$a_1, a_2, \ldots, a_n, \ldots \qquad (0 \leqslant a_n < k).$$

Тогда бесконечный ряд

$$\frac{a_1}{k} + \frac{a_2}{k^2} + \ldots + \frac{a_n}{k^n} + \ldots \tag{1}$$

называется k-ичною дробью (или просто дробью); *исключаются из рассмотрения только такие последовательности, в которых все a_n, начиная с некоторого места, равны $k-1$.*

Обычно такую дробь записывают в известной форме

$$0,a_1a_2 \ldots a_n \ldots$$

Мотивы, заставляющие нас исключить из рассмотрения дроби, оканчивающиеся безграничным повторением цифры $k-1$, хорошо известны из элементарной теории десятичных дробей: число, которое представляется такой дробью, может быть всегда представлено и другой дробью, лишённой этого свойства [1]), и мы добиваемся однозначности в представлении чисел нашими дробями только тогда, если заранее исключаем из рассмотрения одно из этих двух возможных представлений.

Определение 3. *Дробь* (1) *называется конечной, если, начиная с некоторого места, все её цифры равны нулю, и бесконечной в противном случае.*

В обычном начертании конечной дроби стоящие в конце её сплошные нули не выписываются, т. е. вместо $0,a_1\ldots a_n000\ldots$ пишут просто $0,a_1\ldots a_n$.

Так как для любого $n \geqslant 1$

$$0 \leqslant \frac{a_n}{k^n} \leqslant \frac{k-1}{k^n} < \frac{1}{k^{n-1}},$$

то ряд $\sum_{i=1}^{\infty} \frac{a_i}{k^i}$ всегда сходится; другими словами, полагая $s_0 = 0$ и для $n \geqslant 1$

$$s_n = \sum_{i=1}^{n} \frac{a_i}{k^i},$$

мы во всех случаях можем утверждать существование предела

$$\lim_{n \to \infty} s_n = \alpha.$$

Определение 4. *Если* $\sum_{i=1}^{\infty} \frac{a_i}{k^i} = \lim_{n \to \infty} s_n = \alpha$, *то говорят, что дробь* (1) *представляет число* α *или что она равна* α.

Таким образом, всякая k-ичная дробь представляет некоторое действительное число.

Теорема 1. *Если дробь* (1) *представляет число* α, *то для любого* $n \geqslant 0$

$$0 \leqslant \alpha - s_n < \frac{1}{k^n}.$$

---

[1]) Например, в случае десятичных дробей $0{,}1999\ldots = 0{,}2000\ldots$

Примечание. В частности, при $n=0$ мы находим: $0 \leqslant \alpha < 1$; число, представляемое k-ичной дробью, всегда принадлежит, следовательно, этому отрезку.

Доказательство. Так как

$$\alpha - s_n = \sum_{i=n+1}^{\infty} \frac{a_i}{k^i},$$

то, очевидно, $\alpha - s_n \geqslant 0$; далее, так как по нашему соглашению среди цифр $a_{n+1}, a_{n+2}, \ldots$ всегда найдутся меньшие, чем $k-1$, то

$$\alpha - s_n < \sum_{i=n+1}^{\infty} \frac{k-1}{k^i} = \frac{k-1}{k^{n+1}}\left\{1 + \frac{1}{k} + \frac{1}{k^2} + \ldots\right\} = \frac{1}{k^n},$$

чем теорема 1 доказана.

Теорема 2. *Для того чтобы дробь* (1) *представляла число* α, *необходимо и достаточно, чтобы при любом* $n \geqslant 1$ *было*:

$$a_n = [k^n\alpha] - k\,[k^{n-1}\alpha]. \tag{2}$$

Примечание. Символ $[x]$ означает наибольшее целое число, не превосходящее x. Так, $[\pi]=3$, $[-\pi]=-4$ и т. д.

Доказательство. 1) Пусть число α и дробь (1) таковы, что $0 \leqslant \alpha < 1$ и соотношение (2) выполнено для любого $n \geqslant 1$. Тогда

$$s_n = \sum_{i=1}^{n} \frac{a_i}{k^i} = \sum_{i=1}^{n} \frac{[k^i\alpha] - k\,[k^{i-1}\alpha]}{k^i} = \sum_{i=1}^{n}\left\{\frac{[k^i\alpha]}{k^i} - \frac{[k^{i-1}\alpha]}{k^{i-1}}\right\} =$$

$$= \frac{[k^n\alpha]}{k^n} - [\alpha] = \frac{[k^n\alpha]}{k^n},$$

откуда

$$\alpha - s_n = \frac{k^n\alpha - [k^n\alpha]}{k^n}.$$

Но так как для любого x, очевидно, $0 \leqslant x - [x] < 1$, то

$$0 \leqslant \alpha - s_n < \frac{1}{k^n} \qquad (n = 1,\ 2,\ \ldots);$$

отсюда $s_n \to \alpha$ при $n \to \infty$, это и означает, что дробь (1) представляет число α.

2) Пусть теперь, обратно, дробь (1) представляет число α. Тогда в силу теоремы 1 для $n \geqslant 0$

$$0 \leqslant \alpha - s_n < \frac{1}{k^n},$$

откуда

$$k^n s_n \leqslant k^n\alpha < k^n s_n + 1.$$

Но $k^n s_n$ есть целое число; поэтому последние неравенства показывают, что

$$k^n s_n = [k^n \alpha];$$

но при $n \geqslant 1$

$$s_n - s_{n-1} = \frac{a_n}{k^n}, \qquad a_n = k^n (s_n - s_{n-1}),$$

и следовательно,

$$a_n = k^n s_n - k (k^{n-1} s_{n-1}) = [k^n \alpha] - k [k^{n-1} \alpha],$$

чем теорема 2 полностью доказана.

Теорема 3. *Любое действительное число α отрезка $0 \leqslant \alpha < 1$ представляется одной и только одной k-ичной дробью.*

Доказательство. Единственность представления является непосредственным следствием теоремы 2, в силу которой цифры a_n представляющей дроби однозначно выражаются через представляемое число α согласно формулам (2). Что касается возможности представления, то для её доказательства достаточно опять-таки в силу теоремы 2 показать, что числа a_n, определяемые по формулам (2), при любом α могут служить цифрами некоторой k-ичной дроби; а для этого, очевидно, нужно, чтобы для всех $n \geqslant 1$

$$0 \leqslant a_n < k$$

и чтобы все a_n, начиная с некоторого, не оказались равными $k - 1$.

Пусть для $n \geqslant 1$

$$[k^{n-1} \alpha] = g, \quad k^{n-1} \alpha = g + \beta \qquad (0 \leqslant \beta < 1);$$

тогда

$$[k^n \alpha] = [kg + k\beta] = kg + [k\beta]\ ^1),$$

$$k [k^{n-1} \alpha] = kg,$$

так что

$$a_n = [k^n \alpha] - k [k^{n-1} \alpha] = [k\beta];$$

а так как $0 \leqslant \beta < 1$, то

$$0 \leqslant a_n < k.$$

Далее, в силу тех же неравенств $0 \leqslant \beta < 1$ существует такое натуральное число q, что

$$1 - \frac{1}{k^{q-1}} \leqslant \beta < 1 - \frac{1}{k^q};$$

---

[1]) Очевидно, что вообще, если $x = a + y$, где a — целое число, то $[x] = a + [y]$.

отсюда

$$k^{q-1}\beta \geqslant k^{q-1} - 1, \quad k^q\beta < k^q - 1,$$

и следовательно (вспомним, что $k^{n-1}\alpha = g + \beta$),

$$a_{n+q-1} = [k^{n+q-1}\alpha] - k\,[k^{n+q-2}\alpha] = [k^q(g+\beta)] - k\,[k^{q-1}(g+\beta)] =$$
$$= k^q g + [k^q\beta] - k^q g - k\,[k^{q-1}\beta] <$$
$$< k^q - 1 - k(k^{q-1} - 1) = k - 1.$$

Так как при этом n сколь угодно велико, то тем самым доказано, что среди цифр a_i действительно найдётся сколь угодно много таких, которые меньше $k-1$. Этим доказательство теоремы 3 завершено.

Мы видим, таким образом, что систематические дроби при любой системе счисления могут служить формальным аппаратом представления действительных чисел, удовлетворяющим основному требованию возможности и единственности представления для любого действительного числа. Теперь мы должны обратиться к предложениям, устанавливающим связь между арифметической природой представляемого числа и особенностями представляющей его дроби.

Теорема 4. *Всякая периодическая k-ичная дробь представляет некоторое рациональное число α.*

Доказательство. Дробь (1) называется *периодической*, если можно указать такие числа $r \geqslant 0$ и $s \geqslant 1$, что $a_n = a_{n+s}$ для всех $n > r$. Поэтому число α, представляемое такой дробью, может быть записано в виде

$$\alpha = \sum_{i=1}^{\infty} \frac{a_i}{k^i} = \sum_{i=1}^{r} \frac{a_i}{k^i} + \sum_{l=1}^{s} \frac{a_{r+l}}{k^{r+l}} \left\{1 + \frac{1}{k^s} + \frac{1}{k^{2s}} + \dots\right\} =$$
$$= \sum_{i=1}^{r} \frac{a_i}{k^i} + \sum_{l=1}^{s} \frac{a_{r+l}}{k^{r+l}} \cdot \frac{1}{1 - \frac{1}{k^s}},$$

откуда и видно, что α есть рациональное число. Теорема 4 таким образом доказана.

Примечание. Периодическая дробь (1) называется *чисто периодической*, если $r = 0$, и *смешанно-периодической*, если $r > 0$. В случае чисто периодической дроби, т. е. при $r = 0$, последнее равенство даёт для α простое выражение

$$\alpha = \frac{a_1 k^{s-1} + a_2 k^{s-2} + \dots + a_s}{k^s - 1};$$

так как число $k^s - 1$, очевидно, взаимно просто с k, то мы получаем

Дополнение. *Чисто периодическая дробь представляет рациональное число* $\alpha = \frac{a}{b}$, *в котором* b *взаимно просто с* k.

Теорема 5. *Пусть* $\alpha = \frac{a}{b}$ — *такое рациональное число, что* b *взаимно просто с* k. *Тогда* α *представляется чисто периодической дробью.*

Доказательство. Согласно теореме Эйлера (стр. 279), мы имеем:

$$k^{\varphi(b)} \equiv 1 \pmod{b},$$

или, полагая для краткости $\varphi(b) = h$,

$$k^h - 1 = bq,$$

где q — целое число. Поэтому

$$\alpha = \frac{a}{b} = \frac{aq}{bq} = \frac{aq}{k^h - 1} = \frac{aq}{k^h} \cdot \frac{1}{1 - \frac{1}{k^h}} =$$

$$= \frac{aq}{k^h}\left\{1 + \frac{1}{k^h} + \frac{1}{k^{2h}} + \ldots\right\},$$

откуда

$$k^h\alpha = aq\left\{1 + \frac{1}{k^h} + \frac{1}{k^{2h}} + \ldots\right\} = aq + \frac{aq}{k^h}\left\{1 + \frac{1}{k^h} + \frac{1}{k^{2h}} + \ldots\right\} =$$

$$= aq + \alpha$$

и, значит, при любом $n \geqslant 1$

$$a_{n+h} = [k^{n+h}\alpha] - k\,[k^{n+h-1}\alpha] = [k^n(aq + \alpha)] - k\,[k^{n-1}(aq + \alpha)] =$$

$$= k^n aq + [k^n\alpha] - k^n aq - k\,[k^{n-1}\alpha] = [k^n\alpha] - k\,[k^{n-1}\alpha] = a_n.$$

Этим теорема 5 доказана.

Примечание. Из теоремы 5 нельзя заключать, что период дроби, представляющей число α, равен $h = \varphi(b)$; возможно, что период меньше h, так что h последовательных цифр этой дроби содержат не один, а несколько периодов. Вопрос о том, как по данным a и b найти длину периода, представляет значительный интерес, но здесь мы его рассматривать не можем. Это же относится и к аналогичным вопросам, возникающим в связи с теоремой 6.

Теорема 6. *Если* b *не взаимно просто с* k, *то число* $\alpha = \frac{a}{b}$ (*где* a *и* b *взаимно просты*) *представляется смешанно-периодической дробью.*

Доказательство. Пусть число $k^r\alpha = k^r\frac{a}{b}$ имеет несократимую форму $\frac{a'}{b'}$. Если r достаточно велико, то при этом все входящие в b общие множители чисел b и k сократятся, так что мы можем считать b' взаимно простым с k. Пусть $[k^r\alpha] = q$,

$$k^r\alpha = \frac{a'}{b'} = q + \frac{a''}{b'} \qquad \left(0 \leqslant \frac{a''}{b'} < 1\right). \tag{3}$$

В силу теоремы 5 число $\frac{a''}{b'}$ представляется чисто периодической дробью $0,b_1b_2\ldots b_n\ldots$, $b_{n+h} = b_n$ $(n = 1,\ 2,\ldots)$. Но, обозначая через $0,a_1a_2\ldots a_n\ldots$ дробь, представляющую число α, мы будем иметь в силу (2) и (3) для любого $n \geqslant 1$

$$a_{r+n} = [k^{r+n}\alpha] - k\,[k^{r+n-1}\alpha] = \left[k^n\left(q + \frac{a''}{b'}\right)\right] - k\left[k^{n-1}\left(q + \frac{a''}{b'}\right)\right] =$$

$$= \left[k^n\frac{a''}{b'}\right] - k\left[k^{n-1}\frac{a''}{b'}\right] = b_n, \tag{4}$$

откуда

$$a_{r+n+h} = a_{r+n} \qquad (n = 1,\ 2,\ldots).$$

Это показывает, что дробь $0,\ a_1a_2\ldots\ a_n\ldots$, представляющая число $\alpha = \frac{a}{b}$, — периодическая. Она не может быть чисто периодической, так как тогда, в силу дополнения к теореме 4, b было бы взаимно просто с k. Этим теорема 6 доказана.

Примечание. В частности, если все простые множители, содержащиеся в числе b, содержатся и в числе k, то $b' = 1$; а так как $0 \leqslant \frac{a''}{b'} < 1$, то $a'' = 0$ и, следовательно, $b_n = 0$ $(n = 1,\ 2,\ldots)$; но тогда в силу (4) и

$$a_{r+n} = 0 \qquad (n = 1,\ 2,\ldots),$$

т. е. число $\alpha = \frac{a}{b}$ представляется конечной дробью. Очевидно, что справедливо и обратное: всякая конечная дробь представляет рациональное число вида $\alpha = \frac{g}{k}$, где g — целое число; если поэтому несократимая форма дроби α есть $\frac{a}{b}$, то b не может иметь простых делителей, отличных от простых делителей числа k. Поэтому мы получаем

Дополнение. *Для того чтобы число α представлялось конечной k-ичной дробью, необходимо и достаточно, чтобы оно было рационально и чтобы в его несократимой форме $\alpha = \frac{a}{b}$ чи-*

сло b не имело иных простых делителей, кроме простых делителей числа k.

Наконец, совокупность доказанных нами теорем показывает, что все иррациональные числа и только они представляются непериодическими k-ичными дробями. Таким образом, нами установлены теперь все основные законы взаимного соответствия между арифметической природой представляемого числа и типом представляющей его систематической дроби. Важнейший из этих законов состоит в том, что независимо от выбранной системы счисления рациональные числа имеют периодические, а иррациональные — непериодические представления. Дальнейшие особенности представлений рациональных чисел зависят уже, как мы видели, от арифметических связей этих чисел с выбранной системой счисления.

§ 12. Цепные дроби

В главе III мы видели, что всякое рациональное число однозначно представляется цепной дробью $[a_0; a_1, \ldots, a_n]$ и что, обратно, всякая такая дробь представляет некоторое определённое рациональное число. Поэтому, если мы хотим охватить аппаратом цепных дробей и числа иррациональные, то должны, прежде всего, заняться расширением самого этого аппарата. Таким естественным расширением представляется введение бесконечных цепных дробей, т. е. выражений вида

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \ddots}}} = [a_0; a_1, a_2, \ldots, a_n, \ldots], \qquad (5)$$

где a_0 — целое число, а $a_1, a_2, \ldots, a_n, \ldots$ — натуральные числа.

Само собою разумеется, что такого рода выражение не имеет никакого определённого смысла до каких-либо специальных соглашений по этому вопросу [1]).

Чтобы прийти к таким целесообразным соглашениям, заметим, прежде всего, что мы можем для формально определённой дроби (5),

---

[1]) Вспомним, что и аналогичное формальное определение систематической дроби с помощью последовательности цифр $a_1, a_2, \ldots, a_n, \ldots$ также не придавало этому символу определённого реального смысла, покуда мы не согласились приписывать ему значения $\sum_{n=1}^{\infty} \frac{a_n}{k^n}$.

не вкладывая до времени в этот символ никакого реального содержания, построить последовательность «подходящих дробей»

$$\frac{p_0}{q_0}=\frac{a_0}{1},\quad \frac{p_1}{q_1}=a_0+\frac{1}{a_1},$$

$$\frac{p_2}{q_2}=a_0+\frac{1}{a_1+\dfrac{1}{a_2}},\ \ldots,\quad \frac{p_n}{q_n}=a_0+\cfrac{1}{a_1+\cfrac{1}{\ddots+\cfrac{1}{a_n}}},\ \ldots$$

Эти подходящие дроби имеют вполне реальный смысл; они ничем не отличаются от тех подходящих дробей, которые мы рассматривали в главе III, потому что $\frac{p_n}{q_n}$ представляет собою такую функцию элементов $a_0, a_1, \ldots, a_n$, вид которой ни в какой мере не зависит от того, является ли a_n последним элементом или за ним следует ещё a_{n+1}. Всё различие состоит в том, что конечная дробь имеет лишь конечное число таких подходящих дробей, последняя из которых и есть «значение» данной дроби, в то время как бесконечная дробь имеет бесконечную последовательность подходящих дробей, а «значение» её пока ещё нами не определено.

В частности, подходящие дроби обладают следующими свойствами, установленными в главе III:

1. Для $n\geqslant 2$

$$p_n=p_{n-1}a_n+p_{n-2},$$
$$q_n=q_{n-1}a_n+q_{n-2}.$$

2. Для $n\geqslant 0$ дробь $\frac{p_n}{q_n}$ несократима и

$$\Delta_n=q_np_{n+1}-p_nq_{n+1}=(-1)^n.$$

3. С ростом порядка подходящие дроби чётного порядка возрастают, а нечётного — убывают; любая подходящая дробь чётного порядка меньше любой подходящей дроби нечётного порядка.

Перечисленные свойства подходящих дробей дают нам возможность целесообразно определить значение бесконечной цепной дроби и построить развёрнутую теорию таких дробей.

Прежде всего подходящие дроби чётного порядка образуют в силу свойства 3 возрастающую последовательность

$$\frac{p_0}{q_0}<\frac{p_2}{q_2}<\ldots<\frac{p_{2k}}{q_{2k}}<\ldots,$$

все члены которой остаются меньше $\frac{p_1}{q_1}$; поэтому существует предел

$$\lim_{k\to\infty}\frac{p_{2k}}{q_{2k}}=\alpha.$$

Точно так же подходящие дроби нечётного порядка образуют убывающую последовательность

$$\frac{p_1}{q_1} > \frac{p_3}{q_3} > \ldots > \frac{p_{2k+1}}{q_{2k+1}} > \ldots,$$

все члены которой остаются больше чем $\frac{p_2}{q_2}$; поэтому существует предел

$$\lim_{k \to \infty} \frac{p_{2k+1}}{q_{2k+1}} = \beta.$$

Вместе с тем мы имеем для любого $k \geqslant 0$

$$\frac{p_{2k}}{q_{2k}} < \alpha \leqslant \beta < \frac{p_{2k+1}}{q_{2k+1}},$$

и значит,

$$0 \leqslant \beta - \alpha < \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{1}{q_{2k}q_{2k+1}}.$$

Но в силу свойства 1 $q_n > q_{n-1}$ $(n \geqslant 1)$, так что q_n безгранично возрастает при $n \to \infty$. Поэтому правая часть последнего неравенства сколь угодно мала при достаточно большом k; а так как $\beta - \alpha$ от k не зависит, то $\beta = \alpha$.

Таким образом, для каждой бесконечной цепной дроби существует предел

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha,$$

который мы естественно и примем за значение этой дроби. Мы будем также говорить, что бесконечная цепная дробь (5) «представляет» число α; при этом, очевидно, для любого $k \geqslant 0$

$$\frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}}.$$

Далее, отсюда же следует, что при любом $n \geqslant 0$

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}.$$

Так как $\frac{p_n}{q_n} = [a_0;\ a_1,\ a_2, \ldots,\ a_n]$ $(n \geqslant 0)$, то предельное соотношение, связывающее цепную дробь (5) с её подходящими дробями, может быть переписано и в следующей выразительной форме:

$$[a_0;\ a_1,\ a_2,\ \ldots,\ a_n,\ \ldots] = \lim_{n \to \infty} [a_0;\ a_1,\ a_2,\ \ldots,\ a_n].$$

Полученные нами до сих пор результаты мы соберём в следующем предложении:

Теорема 7. *Каждая бесконечная цепная дробь* (5), *в которой* a_0 — *любое целое число, а* $a_1, a_2, \ldots, a_n, \ldots$ — *любые натуральные числа, представляет определённое действительное число* α, *определяемое как*

$$\lim_{n\to\infty}\frac{p_n}{q_n}=\lim_{n\to\infty}[a_0;\ a_1,\ a_2,\ \ldots,\ a_n].$$

При этом для любого $k\geqslant 0$

$$\frac{p_{2k}}{q_{2k}}<\alpha<\frac{p_{2k+1}}{q_{2k+1}},$$

и для любого $n\geqslant 0$

$$\left|\alpha-\frac{p_n}{q_n}\right|<\frac{1}{q_nq_{n+1}}.$$

Во всём предшествующем мы считали дробь (5) данной и искали представляемое ею действительное число α. Теперь мы переходим к решению обратной задачи. Пусть дано любое действительное число α; постараемся узнать, существует ли представляющая это число цепная дробь, и если существует, то сколько таких дробей и как они могут быть найдены.

С этой целью допустим сначала, что число α представляется бесконечной цепной дробью (5), и постараемся выразить через α элементы a_n этой цепной дроби. Так как мы уже знаем (теорема 7), что любая бесконечная цепная дробь представляет некоторое действительное число, то, в частности, мы можем определить числа

$$\alpha_1=[a_1;\ a_2,\ a_3,\ \ldots,\ a_n,\ \ldots],\qquad \alpha_2=[a_2;\ a_3,\ a_4,\ \ldots,\ a_n,\ \ldots],$$

и вообще

$$\alpha_k=[a_k;\ a_{k+1},\ a_{k+2},\ \ldots,\ a_{k+s},\ \ldots]\qquad (k\geqslant 1).$$

Очень легко установить соотношение между числами α_k и α_{k+1}. В самом деле, условимся обозначать через $\frac{u_r}{v_r}$ подходящие дроби той цепной дроби, которая определяет α_k, и через $\frac{u_r'}{v_r'}$ — той, которая определяет α_{k+1}; тогда

$$\frac{u_r}{v_r}=[a_k;\ a_{k+1},\ a_{k+2},\ \ldots,\ a_{k+r}]=a_k+\frac{1}{[a_{k+1};\ a_{k+2},\ \ldots,\ a_{k+r}]}=$$

$$=a_k+\frac{1}{\dfrac{u_{r-1}'}{v_{r-1}'}}.$$

Так как по определению α_k и α_{k+1}

$$\lim_{r\to\infty}\frac{u_r}{v_r}=\alpha_k,\qquad \lim_{r\to\infty}\frac{u_{r-1}'}{v_{r-1}'}=\alpha_{k+1},$$

то, заставляя в полученном равенстве r безгранично возрастать (при неизменном k), мы в пределе находим (если положить $\alpha_0 = \alpha$)

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}} \qquad (k \geqslant 0). \tag{6}$$

Так как при $k \geqslant 1$ и $a_k \geqslant 1$, то $\alpha_k > 1$ для $k = 1, 2, \ldots$ Поэтому соотношения (6) (где $\frac{1}{\alpha_{k+1}} < 1$) дают:

$$a_k < \alpha_k < a_k + 1 \qquad (k \geqslant 0);$$

а это означает, что

$$a_k = [\alpha_k] \qquad (k \geqslant 0). \tag{7}$$

Таким образом, если число α представляется какой-либо бесконечной цепной дробью (5), то элементы этой дроби могут быть рекуррентно найдены следующим простым процессом: 1) $a_0 = [\alpha]$; 2) если числа α_i и a_i уже найдены для $i \leqslant k$, то α_{k+1} определяется соотношением (6), а затем a_{k+1} определяется в силу (7) как $[\alpha_{k+1}]$.

Мы приходим, таким образом, к чрезвычайно важному выводу: если число α может быть представлено бесконечной цепной дробью, то элементы этой дроби по числу α определяются однозначно. Это показывает, что представление числа α в виде бесконечной цепной дроби, если оно существует, является единственным; другими словами, *не может существовать двух различных бесконечных цепных дробей, представляющих одно и то же число.*

Заметим теперь, что в случае, когда число $\alpha = \frac{a}{b}$ рационально, наш процесс последовательного построения чисел $\alpha_1, \alpha_2, \ldots$, выражаемый рекуррентной формулой (6), ничем не отличается от того процесса, с помощью которого мы в главе III (стр. 297) разлагали число $\frac{a}{b}$ в цепную дробь, и наши числа $\alpha_0, \alpha_1, \alpha_2, \ldots$ — не что иное, как построенные там числа $\frac{a}{b}, \frac{b}{r_1}, \frac{r_1}{r_2}, \ldots$ Но там мы видели, что в случае рационального $\alpha = \frac{a}{b}$ этот разряд чисел необходимо о б р ы в а е т с я, т. е. одно из чисел $\alpha_k = \frac{r_{k-1}}{r_k}$ оказывается целым, так что $a_k = \alpha_k$, и α_{k+1} по формуле (6) уже не может быть определено. Теперь же мы видим, что если число α может быть представлено бесконечной цепной дробью, то для него процесс, определяемый соотношением (6), никогда не может закончиться и продолжается безгранично. Из этого сопоставления вытекает, очевидно, что ни одно рациональное число не может быть представлено бесконечной цепной дробью и что, следовательно, *все числа, представляемые бесконечными цепными дробями, иррациональны.*

Чтобы завершить этот круг исследований, нам остаётся показать, что всякое иррациональное число действительно может быть пред-

ставлено бесконечной цепной дробью (единственность такого представления нами уже установлена). Пусть α — любое иррациональное число; определим для него последовательности чисел α_k и a_k вышеописанным рекуррентным процессом, т. е. с помощью соотношений (6) и (7) (этот процесс будет обязательно бесконечным, так как оборваться он мог бы только, если бы какое-нибудь α_n оказалось целым числом; но тогда, очевидно, число α было бы рациональным); при этом мы имеем:

$$0 < \frac{1}{\alpha_{k+1}} = \alpha_k - a_k = \alpha_k - [\alpha_k] < 1,$$

и следовательно, $\alpha_{k+1} > 1$, а значит, и $a_{k+1} \geqslant 1$ для $k \geqslant 0$.

Как мы видели выше, при любом $n \geqslant 0$

$$\alpha = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\alpha_{n+1}}}},$$

$$\frac{p_{n+1}}{q_{n+1}} = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}.$$

Эти соотношения показывают, что если в выражении подходящей дроби $\frac{p_{n+1}}{q_{n+1}}$ как функции от $a_0, a_1, \ldots, a_n, a_{n+1}$ заменить a_{n+1} через α_{n+1} (не изменяя $a_0, a_1, \ldots, a_n$), то значение этой функции будет равно α. А так как

$$\frac{p_{n+1}}{q_{n+1}} = \frac{p_n a_{n+1} + p_{n-1}}{q_n a_{n+1} + q_{n-1}},$$

где $p_{n-1}, p_n, q_{n-1}, q_n$ зависят только от $a_0, a_1, \ldots, a_n$, то

$$\alpha = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}}; \tag{8}$$

отсюда

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}} - \frac{p_n}{q_n}\right| =$$

$$= \frac{|q_n p_{n-1} - p_n q_{n-1}|}{(q_n \alpha_{n+1} + q_{n-1}) q_n} = \frac{1}{(q_n \alpha_{n+1} + q_{n-1}) q_n} < \frac{1}{q_n^2}.$$

Таким образом,

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha,$$

т. е. построенная нами бесконечная цепная дробь действительно представляет данное иррациональное число α.

Общий вывод, к которому мы пришли, может быть формулирован в виде следующего основного предложения:

Теорема 8. *Каждое действительное число α единственным образом представляется цепною дробью; эта дробь конечна, если число α рационально, и бесконечна, если оно иррационально.*

При этом важно отметить, что проведённое нами доказательство носит вполне конструктивный характер, т. е. устанавливает не только самый факт существования представляющей данное число цепной дроби, но и метод, позволяющий с помощью весьма простого алгорифма последовательно найти все её элементы.

Мы видим, что основной закон представления чисел цепными дробями, выражаемый теоремами 7 и 8, замечательно прост: каждому числу соответствует единственная дробь, каждой дроби — единственное число; рациональным числам соответствуют конечные, иррациональным — бесконечные дроби. Как мы уже подчёркивали, такая стройность и простота обусловлены свойствами самого аппарата и, прежде всего, — его «абсолютным» характером, не связанным ни с какой определённой системой счисления.

Независимо от введения элементов теории цепных дробей в наши школьные программы это учение даёт превосходный материал для кружковой и вообще внеклассной работы. В этом отношении можно особенно рекомендовать содержание следующей главы 5. Опыт показывает, что цепные дроби и их использование для приближённого представления действительных чисел всегда привлекают внимание и интерес учащихся; в особенности это касается тех случаев, когда результаты формулируются в виде простых, законченных и эффектных теорем, к тому же легко и изящно доказываемых, как это имеет место почти во всей проблематике, связанной с представлением чисел цепными дробями.

ГЛАВА V

ЦЕПНЫЕ ДРОБИ И ДИОФАНТОВЫ ПРИБЛИЖЕНИЯ

§ 13. Подходящие дроби в роли наилучших приближений

Если хотят приближённо выразить какое-либо действительное число с помощью рациональной дроби, то на практике с этой целью обычно пользуются аппаратом десятичных дробей. Данное число (будет ли оно рациональным или иррациональным) разлагается в десятичную дробь; если эта дробь оказывается конечной и притом не длинной, то, конечно, никаких приближений искать не приходится, так как полученная несложная десятичная дробь даёт удобное и притом абсолютно точное представление данного числа. Но если получаемая десятичная дробь окажется бесконечной или хотя бы и конечной, но слишком длинной и потому неудобной для практических расчётов, то для целей практики её по известным правилам «округляют», т. е. ограничивают небольшим числом десятичных знаков, отбрасывая остальные. Такое «округление» и есть не что иное, как замена ценою некоторой погрешности данного числа рациональной дробью со сравнительно небольшими числителем и знаменателем.

Какова же допускаемая при этом погрешность? Так как наша цель при всяком таком приближённом представлении состоит в том, чтобы получить возможно бо́льшую точность (т. е. возможно меньшую погрешность) при возможно меньших числителе и знаменателе приближающей дроби, то естественно, что величину погрешности обычно сравнивают с величиной знаменателя этой дроби (конечно, числитель и знаменатель этой дроби имеют один и тот же порядок великости, так что для сравнения достаточно привлечь какое-нибудь одно из этих чисел; знаменателя выбирают потому, что его всегда считают положительным, тогда как числитель может быть и отрицательным). Если при округлении данной десятичной дроби мы ограничиваемся n знаками после запятой, то это означает, что данное число приближённо представляется дробью со знаменателем $q = 10^n$. Как известно, погрешность при этом не превосходит половины единицы последнего из взятых нами разрядов, т. е. не превосходит

$$\frac{1}{2 \cdot 10^n} = \frac{1}{2q}.$$

Сравним теперь этот результат с тем, что даёт аппарат цепных дробей. Если $\frac{p}{q}$ есть одна из подходящих дробей данного числа α, то, как мы знаем (см. теорему 7 главы IV),

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qq'}, \tag{1}$$

где q' — знаменатель следующей за $\frac{p}{q}$ подходящей дроби. Так как $q' > q$, то тем более

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2};$$

таким образом, заменяя в порядке приближения число α подходящей дробью $\frac{p}{q}$, мы допускаем погрешность, не превосходящую $\frac{1}{q^2}$. При сколько-нибудь значительном q величина $\frac{1}{q^2}$ во много раз меньше, чем $\frac{1}{2q}$; это показывает, что приближение подходящими дробями при примерно одинаковом порядке знаменателя приближающей дроби даёт погрешность, во много раз меньшую, чем приближение десятичными (и вообще систематическими) дробями.

Рассмотрим пример. Пусть мы хотим найти приближённое значение числа π в виде рациональной дроби, знаменатель которой не превосходил бы 100. Известно, что разложение в десятичную дробь даёт нам ответ в виде дроби

$$3{,}14 = \frac{314}{100}$$

с погрешностью, приблизительно равной 0,0016.

С другой стороны, разлагая π в цепную дробь, легко находим:

$$\pi = [3;\ 7,\ 15,\ \ldots];$$

это даёт:

$$\frac{p_0}{q_0} = \frac{3}{1},\quad \frac{p_1}{q_1} = \frac{22}{7},\quad \frac{p_2}{q_2} = \frac{333}{106};$$

так как знаменатель приближающей дроби должен быть не больше 100, то мы выбираем в качестве приближения дробь $\frac{22}{7}$ и получаем в силу неравенства (1)

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{7 \cdot 106} < 0{,}0014.$$

Мы видим, таким образом, что приближение подходящей дробью дало нам лучшую точность при значительно меньшем знаменателе (7 вместо 100), чем приближение десятичной дробью. Мы видим наглядно, чем это вызывается: когда мы приближаем данное число десятичной дробью, мы можем выбирать знаменатель только вида 10^n; поэтому при выборе этого знаменателя мы бессильны учесть

арифметическую природу представляемого числа: если бы в нашем примере мы вместо π искали приближённого представления для любого другого числа, знаменатель приближающей дроби остался бы всё тот же — 100. Напротив, при аппроксимации подходящими дробями мы выбираем знаменатель приближающей дроби, исходя из разложения данного числа в цепную дробь, т. е. всемерно учитывая его арифметическую природу; для различных представляемых чисел знаменатели при этом окажутся весьма различными; и естественно, что эта гораздо бóльшая свобода маневрирования приводит к значительно лучшим результатам. Мы видим, таким образом, что за те действительно замечательные вычислительные удобства, которые предоставляют нам систематические дроби, нам приходится расплачиваться довольно дорогой ценой.

Если, таким образом, сравнение качества систематических и цепных дробей как приближающего аппарата решительно говорит в пользу цепных дробей, то всё же оценка эта является, конечно, лишь сравнительной, и остаётся открытым вопрос о возможности ещё более сильных методов. Поэтому мы теперь займёмся изучением доброкачественности приближений, даваемых подходящими дробями, с абсолютной точки зрения, безотносительно к другим специальным приближающим аппаратам. Прежде всего мы убедимся, что подходящие дроби данного числа являются для него «наилучшими приближениями» в следующем совершенно определённом смысле:

Теорема 1. *Если* $\frac{p_n}{q_n}$ *— подходящая дробь числа* α, *то любая дробь* $\frac{p}{q}$, *знаменатель которой* $q < q_n$, *отстоит от* α *дальше, чем* $\frac{p_n}{q_n}$.

Таким образом, любая подходящая дробь даёт нам приближение, лучшее, чем любая дробь с меньшим знаменателем, так что всякое дальнейшее усиление точности может быть достигнуто лишь ценою увеличения знаменателя (а значит, и числителя) приближающей дроби.

Для доказательства этой теоремы убедимся сначала, что всякая подходящая дробь $\frac{p_n}{q_n}$ лежит к α ближе, чем предшествующая подходящая дробь $\frac{p_{n-1}}{q_{n-1}}$. В самом деле, в силу теоремы 7 главы IV (стр. 318) дробь $\frac{p_{n+1}}{q_{n+1}}$ лежит между $\frac{p_{n-1}}{q_{n-1}}$ и α; поэтому

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| > \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_{n-1}}{q_{n-1}}\right| =$$

$$= \frac{|q_{n-1}(p_n a_{n+1} + p_{n-1}) - p_{n-1}(q_n a_{n+1} + p_{n-1})|}{q_{n-1} q_{n+1}} =$$

$$= \frac{a_{n+1}}{q_{n-1} q_{n+1}} > \frac{1}{q_n q_{n+1}} > \left|\alpha - \frac{p_n}{q_n}\right|, \qquad (2)$$

что мы и утверждали.

Теперь мы должны показать, что если $0<q<q_n$, то

$$\left|\alpha-\frac{p}{q}\right|>\left|\alpha-\frac{p_n}{q_n}\right|. \tag{3}$$

Если $\frac{p}{q}=\frac{p_{n-1}}{q_{n-1}}$, то неравенство (3) совпадает с уже доказанным нами неравенством (2). Поэтому допустим, что $\frac{p}{q}\neq\frac{p_{n-1}}{q_{n-1}}$. Тогда

$$\left|\frac{p}{q}-\frac{p_{n-1}}{q_{n-1}}\right|=\frac{|pq_{n-1}-qp_{n-1}|}{qq_{n-1}}\geqslant\frac{1}{qq_{n-1}}>\frac{1}{q_nq_{n-1}}>\left|\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right|,$$

т. е. $\frac{p}{q}$ отстоит от $\frac{p_{n-1}}{q_{n-1}}$ дальше, чем $\frac{p_n}{q_n}$, и потому не может принадлежать отрезку $\left(\frac{p_{n-1}}{q_{n-1}},\ \frac{p_n}{q_n}\right)$, внутри которого, как мы знаем, лежит α. Таким образом, либо $\frac{p}{q}$ лежит относительно α по ту же сторону, что $\frac{p_n}{q_n}$, но дальше, чем $\frac{p_n}{q_n}$; тогда

$$\left|\alpha-\frac{p}{q}\right|>\left|\alpha-\frac{p_n}{q_n}\right|,$$

что и требовалось доказать; либо же $\frac{p}{q}$ лежит относительно α по ту же сторону, что $\frac{p_{n-1}}{q_{n-1}}$, но дальше, чем $\frac{p_{n-1}}{q_{n-1}}$; тогда

$$\left|\alpha-\frac{p}{q}\right|>\left|\alpha-\frac{p_{n-1}}{q_{n-1}}\right|>\left|\alpha-\frac{p_n}{q_n}\right|.$$

Теорема 1, таким образом, доказана во всех случаях.

До сих пор мы всегда измеряли доброкачественность приближения числа α дробью $\frac{p}{q}$ тем, насколько мала разность $\left|\alpha-\frac{p}{q}\right|$; такой подход является, конечно, наиболее естественным. Однако во многих случаях мы можем использовать с этой целью и величину $|q\alpha-p|$, отличающуюся от предыдущей лишь множителем q. Так, например, найденный нами для любой подходящей дроби $\frac{p_n}{q_n}$ числа α закон приближения

$$\left|\alpha-\frac{p_n}{q_n}\right|<\frac{1}{q_nq_{n+1}}$$

может быть, конечно, с тою же точностью выражен неравенством

$$|q_n\alpha-p_n|<\frac{1}{q_{n+1}}.$$

В этом случае указанный выше переход оказывается вполне тривиальным. Однако история развития всего этого учения показала, что систематическое использование величины $|q\alpha - p|$ для оценки приближения числа α рациональной дробью $\frac{p}{q}$ имеет заметные преимущества перед применением с этой целью величины $\left|\alpha - \frac{p}{q}\right|$. С одной стороны, законы приближения часто находят себе при этом более цельное и законченное выражение (пример такого случая мы сейчас увидим); с другой стороны (и это особенно важно), этот путь оказывается чрезвычайно богатым расширяющими возможностями: с предельной естественностью он ведёт к образованию новых понятий и постановке новых задач, в значительной степени обогащающих собою эту область науки. В дальнейшем мы будем иметь случай указать некоторые примеры и в этом направлении.

Попытаемся, прежде всего, рассмотреть с этой новой точки зрения ту задачу, решение которой в нашей прежней трактовке даётся теоремой 1. Пусть $\frac{p_n}{q_n}$ — подходящая дробь числа α и пусть $0 < q < q_n$; можно ли тогда утверждать, что при любом целом p

$$|q\alpha - p| > |q_n\alpha - p_n| ? \tag{4}$$

Для решения этого вопроса мы рассмотрим систему двух уравнений

$$\left.\begin{aligned} p_n x + p_{n+1} y &= p, \\ q_n x + q_{n+1} y &= q \end{aligned}\right\} \tag{5}$$

с неизвестными x и y; так как $p_n q_{n+1} - q_n p_{n+1} = \pm 1$, то системе этой удовлетворяет единственная пара чисел (x, y) и эти числа — целые. Несколько расширяя наши предпосылки, мы допустим, что q есть любое натуральное число, меньшее, чем q_{n+1} и отличное от q_n; с другой стороны, мы, очевидно, можем, не ограничивая общности поставленной задачи, допустить, что дробь $\frac{p}{q}$ несократима. Тогда легко убедиться, что определяемые системой (5) целые числа x и y будут иметь противоположные знаки, т. е. $xy < 0$. В самом деле, если $xy > 0$ или $x = 0$, то второе из уравнений (5) даёт $q \geqslant q_{n+1}$, что неверно; если же $y = 0$, то мы из этого же уравнения получаем $q = q_n$, что также исключено (разумеется, в этом случае $x = 1$, так как иначе дробь $\frac{p}{q}$ не была бы несократимой). Итак, $xy < 0$.

Но из уравнений (5) следует:

$$q\alpha - p = x(q_n\alpha - p_n) + y(q_{n+1}\alpha - p_{n+1}).$$

Так как числа $q_n\alpha - p_n$ и $q_{n+1}\alpha - p_{n+1}$ в силу теоремы 7 главы IV имеют противоположные знаки, то из $xy < 0$ следует, что оба сла-

гаемых правой части последнего равенства имеют один и тот же знак, вследствие чего

$$|q\alpha - p| = |x| \cdot |q_n\alpha - p_n| + |y| \cdot |q_{n+1}\alpha - p_{n+1}|.$$

Отсюда мы имеем неравенство (4) во всех случаях, кроме одного только исключения: если $q_{n+1}\alpha - p_{n+1} = 0$, $|x| = 1$, то

$$|q\alpha - p| = |q_n\alpha - p_n|.$$

При этом уравнения (5) дают обязательно:

$$x = -1, \quad y = 1, \quad q = q_{n+1} - q_n, \quad p = p_{n+1} - p_n.$$

Итак, мы приходим к выводу, что при $0 < q < q_{n+1}$ всегда

$$|q\alpha - p| \geqslant |q_n\alpha - p_n|;$$

при этом знак равенства возможен только в случае, когда $q = q_n$, или в случае, когда $\alpha = \frac{p_{n+1}}{q_{n+1}}$, $q = q_{n+1} - q_n = (a_{n+1} - 1)\,q_n + q_{n-1}$; в этом последнем случае a_{n+1}, будучи последним элементом конечной цепной дроби

$$[a_0;\ a_1,\ a_2,\ \ldots,\ a_{n+1}] = \alpha,$$

по нашему соглашению (глава III, стр. 300) всегда больше единицы, так что $q \geqslant q_n + q_{n-1} > q_n$.

Таким образом, мы находим:

$$|q\alpha - p| > |q_n\alpha - p_n| \qquad (0 < q < q_n), \tag{6}$$

$$|q\alpha - p| \geqslant |q_n\alpha - p_n| \qquad (0 < q < q_{n+1}). \tag{7}$$

Условимся называть рациональную дробь $\frac{l}{k}$ *наилучшим приближением второго рода числа* α, если при $0 < k' < k$ и любом целом l'

$$|k'\alpha - l'| > |k\alpha - l|.$$

Неравенство (6) показывает, что всякая подходящая дробь числа α служит для него наилучшим приближением второго рода; слова «второго рода» имеют целью указать, что здесь близость дроби $\frac{l}{k}$ к числу α мы оцениваем разностью $|k\alpha - l|$ в противоположность приближениям «первого рода», о которых говорит теорема 1, и где близость оценивается разностью $\left|\alpha - \frac{l}{k}\right|$.

Таким образом, подходящие дроби оказываются «наилучшими приближениями» как в том, так и в другом смысле. Замечательно, однако, что в случае приближений второго рода подходящие дроби обладают этим свойством, так сказать, монопольно: *всякое наилучшее приближение второго рода есть подходящая дробь.*

В самом деле, если дробь $\frac{p}{q}$ не есть подходящая дробь числа α, то пусть n таково, что $q_n < q < q_{n+1}$ [1]); так как в силу неравенства (7) тогда

$$|q_n\alpha - p_n| \leqslant |q\alpha - p| \qquad (q_n < q),$$

то $\frac{p}{q}$ не может служить наилучшим приближением второго рода для числа α. Таким образом, мы можем считать установленным следующее предложение:

Теорема 2. *Все подходящие дроби данного числа и только они являются наилучшими приближениями второго рода.*

Можно было бы показать, что теорема 1 не допускает обращения, подобного только что проведённому: кроме подходящих дробей, в качестве наилучших приближений первого рода могут выступать и другие дроби. Таким образом, мы в рассматриваемом случае как раз имеем пример такого положения вещей, когда рассмотрение разностей типа $|q\alpha - p|$ приводит к результатам более простым и законченным, чем для разностей типа $\left|\alpha - \frac{p}{q}\right|$.

Вместе с тем теорема 2 естественно ставит перед нами и одну новую задачу. Пусть нам даны действительное число α и рациональная дробь $\frac{p}{q}$; как узнать, будет ли $\frac{p}{q}$ подходящей дробью числа α? В известном смысле теорема 2 на этот вопрос отвечает: надо посмотреть, будет ли дробь $\frac{p}{q}$ для числа α наилучшим приближением второго рода. Однако такой ответ нас мало удовлетворяет, так как этим путём нам придётся сравнивать данную дробь со всеми дробями, имеющими меньшие знаменатели; мы естественно хотим иметь такие признаки, которые позволили бы нам решить поставленный вопрос, привлекая к рассмотрению только число α и данную дробь $\frac{p}{q}$.

Пример замечательно простого признака такого рода даёт нам доказанная ещё Лежандром

Теорема 3. *Если* $q > 0$ *и*

$$|q\alpha - p| \leqslant \frac{1}{2q},$$

то $\frac{p}{q}$ *есть подходящая дробь числа* α.

---

[1]) Случай $q = q_n$, $p \neq p_n$ мы можем не рассматривать; легко видеть, что такая дробь $\frac{p}{q}$ не может быть наилучшим приближением второго рода, так как, например, при $q = q_n > 1$, $p \neq p_n$, $|q\alpha - p| = |(q_n\alpha - p_n) + (p_n - p)| \geqslant 1 - |q_n\alpha - p_n| > 1 - \frac{1}{q_{n+1}} > \frac{1}{q_n} > |q_{n-1}\alpha - p_{n-1}|$.

Воспользовавшись теоремой 2, мы можем так сформулировать теорему 3: *если* $q>0$ *и*

$$|q\alpha-p|\leqslant\frac{1}{2q},$$

то $\frac{p}{q}$ *является наилучшим приближением числа* α.

Доказательство. Пусть дана рациональная дробь $\frac{p'}{q'}$ такая, что

$$q'>0 \quad \text{и} \quad |q'\alpha-p'|\leqslant|q\alpha-p|\leqslant\frac{1}{2q}. \qquad \text{(а)}$$

Для доказательства теоремы достаточно убедиться в том, что $q'\geqslant q$. В самом деле, из неравенств (а) имеем:

$$\left|\alpha-\frac{p'}{q'}\right|\leqslant\frac{1}{2qq'}, \quad \left|\alpha-\frac{p}{q}\right|\leqslant\frac{1}{2q^2};$$

в предположении $q\neq q'$ $\left(\text{и, следовательно, } \frac{p}{q}\neq\frac{p'}{q'}, |p'q-q'p|\geqslant 1\right)$ отсюда вытекает:

$$\frac{1}{qq'}\leqslant\left|\frac{p'}{q'}-\frac{p}{q}\right|\leqslant\left|\frac{p'}{q'}-\alpha\right|+\left|\alpha-\frac{p}{q}\right|\leqslant\frac{1}{2qq'}+\frac{1}{2q^2},$$

откуда

$$\frac{1}{q'}\leqslant\frac{1}{2q'}+\frac{1}{2q}, \quad \frac{1}{2q'}\leqslant\frac{1}{2q},$$

т. е. $q'\leqslant q$, что и требовалось доказать.

Теорема 3 даёт очень простой признак того, что дробь $\frac{p}{q}$ есть одна из подходящих дробей числа α; однако признак этот не является характеристическим: число α может, вообще говоря, иметь бесчисленное множество подходящих дробей, не обладающих этим признаком. Можно было бы убедиться, что вообще необходимого и достаточного признака вида

$$|q\alpha-p|<\frac{a}{q},$$

где a — постоянное число, существовать не может.

Можно, однако, всё же указать для подходящих дробей числа α характеристический (т. е. необходимый и достаточный) критерий достаточно простого вида. Разложим данную дробь $\frac{p}{q}$ в цепную дробь

$$\frac{p}{q}=[a_0;\ a_1,\ a_2,\ \ldots,\ a_n]$$

и обозначим через $\frac{p'}{q'}$ предпоследнюю подходящую дробь этого разложения:

$$\frac{p'}{q'}=[a_0;\ a_1,\ a_2,\ \ldots,\ a_{n-1}].$$

Тогда имеет место следующая теорема, также принадлежащая Лежандру:

Теорема 4. *Для того чтобы дробь* $\frac{p}{q}$ *была подходящей дробью числа* α, *необходимо и достаточно, чтобы*

$$|q\alpha - p| < \frac{1}{q+q'}. \tag{8}$$

Примечание. Так как всегда $q+q' < 2q$, то теорема 3 является непосредственным следствием теоремы 4.

Доказательство. 1) Если $\frac{p}{q}$ есть подходящая дробь числа α, то $\frac{p'}{q'}$ есть предшествующая подходящая дробь; как мы видели много раз, при этом [1])

$$|q\alpha - p| < \frac{1}{q''},$$

где q'' есть знаменатель следующей за $\frac{p}{q}$ подходящей дроби. Но в силу закона образования подходящих дробей q'' может быть представлено в виде $aq+q'$, где $a \geqslant 1$, и следовательно, $q'' \geqslant q+q'$, так что

$$|q\alpha - p| < \frac{1}{q+q'};$$

необходимость признака, таким образом, установлена.

2) Пусть теперь, обратно, имеет место неравенство (8). Мы всегда можем (и притом единственным образом) определить действительное число β так, что

$$\alpha = \frac{p\beta + p'}{q\beta + q'} \tag{9}$$

(для этого достаточно решить написанное уравнение относительно β). Пусть разложение числа β в цепную дробь есть $\beta = [a_{n+1}; a_{n+2}, \ldots]$; покажем, что $a_{n+1} \geqslant 1$, для чего достаточно убедиться, что $\beta \geqslant 1$.

Согласно неравенству (8)

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{p\beta + p'}{q\beta + q'} - \frac{p}{q}\right| = \frac{1}{q(q\beta + q')} < \frac{1}{q(q+q')},$$

откуда

$$q\beta + q' > q + q'$$

и, следовательно, $\beta > 1$.

---

[1]) Мы предполагаем здесь $q\alpha \neq p$; это не ограничивает общности, так как при $q\alpha = p$ неравенство (8) тривиально.

Так как мы знаем [глава IV, стр. 320, формула (8)], что из

$$\frac{p}{q}=[a_0;\ a_1,\ \ldots,\ a_n]$$

следует:

$$\frac{p\beta+p'}{q\beta+q'}=[a_0;\ a_1,\ \ldots,\ a_n,\ \beta]\ ^{1}),$$

то

$$\alpha=[a_0;\ a_1,\ \ldots,\ a_n,\ \beta].$$

Пусть теперь подходящие дроби числа β будут:

$$\frac{p_s'}{q_s'}=[a_{n+1};\ a_{n+2},\ \ldots,\ a_{n+s}];$$

тогда

$$\beta=\lim_{s\to\infty}\frac{p_s'}{q_s'}$$

и

$$\alpha=\lim_{s\to\infty}\left[a_0;\ a_1,\ \ldots,\ a_n,\ \frac{p_s'}{q_s'}\right]=$$

$$=\lim_{s\to\infty}[a_0;\ a_1,\ \ldots,\ a_n,\ a_{n+1},\ \ldots,\ a_{n+s}].$$

Но это означает, что α равно цепной дроби

$$[a_0;\ a_1,\ \ldots,\ a_n,\ a_{n+1},\ \ldots],$$

все элементы которой, как мы доказали, положительны; эта дробь и есть, как мы знаем, единственная цепная дробь, представляющая число α; в частности,

$$\frac{p}{q}=[a_0;\ a_1,\ \ldots,\ a_n]$$

есть подходящая дробь числа α, чем доказана и достаточность признака Лежандра.

Мы уже говорили выше, что признак, даваемый теоремой 3, не является необходимым (или, что то же, теорема 3 не допускает обращения). Но если не каждая подходящая дробь обладает этим признаком, то всё же из каждых двух последовательных подходящих дробей числа α по меньшей мере одна им обладает; об этом говорит следующая, установленная Валеном

Теорема 5. *Если* $\frac{p}{q}$ *и* $\frac{p'}{q'}$ *— две последовательные подходящие дроби числа* α, *то имеет место по меньшей мере одно из двух неравенств*

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2},\quad \left|\alpha-\frac{p'}{q'}\right|<\frac{1}{2q'^2}.$$

---

[1]) Здесь число β, вообще говоря, не целое; разумеется, это ни в какой мере не должно смущать читателя, так как данное нами определение символа $[a_0, a_1, a_2, \ldots, a_n, \beta]$ сохраняет смысл при любом $\beta\neq 0$.

Доказательство. Так как дроби $\frac{p}{q}$ и $\frac{p'}{q'}$ лежат по разные стороны числа α, то из

$$\left|\alpha-\frac{p}{q}\right|\geqslant\frac{1}{2q^2},\quad\left|\alpha-\frac{p'}{q'}\right|\geqslant\frac{1}{2q'^2}$$

следовало бы:

$$\left|\frac{p'}{q'}-\frac{p}{q}\right|=\frac{1}{qq'}\geqslant\frac{1}{2}\left(\frac{1}{q^2}+\frac{1}{q'^2}\right),$$

или

$$\frac{1}{q^2}+\frac{1}{q'^2}-\frac{2}{qq'}=\left(\frac{1}{q}-\frac{1}{q'}\right)^2\leqslant 0,$$

что очевидно неверно. Этим теорема 5 доказана.

Таким образом, всякое иррациональное число α имеет бесконечное множество таких подходящих дробей $\frac{p}{q}$, что

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}.$$

Сам собою встаёт здесь вопрос о возможности усиления этого результата: нельзя ли заменить здесь постоянную $^1/_2$ в правой части неравенства другою, меньшей постоянной c, которая выполняла бы ту же самую роль, т. е. для любого иррационального числа α существовало бы бесчисленное множество таких подходящих дробей $\frac{p}{q}$, что

$$\left|\alpha-\frac{p}{q}\right|<\frac{c}{q^2}\ ?$$

И если такие числа $c<\frac{1}{2}$ существуют, то каково наименьшее из них? Решение этого вопроса означает в известном смысле отыскание наилучшего универсального (т. е. имеющего место для любой иррациональности α) закона приближения действительных чисел рациональными дробями.

Гурвиц доказал, что наименьшее допустимое значение постоянной c есть $\frac{1}{\sqrt{5}}$. Несколько позднее Борель показал, что из любых трёх последовательных подходящих дробей любого числа α по меньшей мере одна даёт требуемое приближение; таким образом, имеет место

Теорема 6. *Если* $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}, \frac{p_{n+2}}{q_{n+2}}$ — *три последовательные подходящие дроби числа* α, *то имеет место по меньшей мере одно из трёх неравенств*

$$\left|\alpha-\frac{p_n}{q_n}\right|<\frac{1}{\sqrt{5}\,q_n^2},\quad\left|\alpha-\frac{p_{n+1}}{q_{n+1}}\right|<\frac{1}{\sqrt{5}\,q_{n+1}^2},$$

$$\left|\alpha-\frac{p_{n+2}}{q_{n+2}}\right|<\frac{1}{\sqrt{5}\,q_{n+2}^2}.$$

Если же $c<\frac{1}{\sqrt{5}}$, *то можно найти такое иррациональное число* α, *что неравенству*

$$\left|\alpha-\frac{p}{q}\right|<\frac{c}{q^2}$$

будет удовлетворять не более конечного числа рациональных дробей $\frac{p}{q}$.

Доказательство. Для доказательства первого утверждения теоремы 6 нам понадобится следующая

Лемма. *Из двух отношений* $\frac{q_{n+1}}{q_n}$ *и* $\frac{q_{n+2}}{q_{n+1}}$ *по меньшей мере одно превосходит число* $\gamma=\frac{\sqrt{5}+1}{2}$.

В самом деле, из $\frac{q_{n+1}}{q_n}<\gamma$, $\frac{q_{n+2}}{q_{n+1}}<\gamma$ [1]) в силу $1+\frac{1}{\gamma}=\gamma$ следовало бы:

$$\gamma>\frac{q_{n+2}}{q_{n+1}}=a_{n+2}+\frac{q_n}{q_{n+1}}>1+\frac{1}{\gamma}=\gamma;$$

этим лемма доказана.

Положим теперь для любого $i\geqslant 1$

$$\psi_i=\alpha_{i+1}+\frac{q_{i-1}}{q_i},$$

где

$$\alpha_{i+1}=[a_{i+1};\ a_{i+2},\ a_{i+3},\ldots]$$

имеет тот же смысл, что и в главе IV (см. стр. 318). Как мы там видели (стр. 320),

$$\left|\alpha-\frac{p_i}{q_i}\right|=\frac{1}{q_i(q_i\alpha_{i+1}+q_{i-1})}=\frac{1}{\psi_i q_i^2};$$

поэтому наше утверждение будет доказано, если покажем, что по меньшей мере одно из трёх чисел ψ_n, ψ_{n+1}, ψ_{n+2} превосходит $\sqrt{5}$.

Так как $\alpha_{i+1}=a_{i+1}+\frac{1}{\alpha_{i+2}}$ и $\frac{q_{i+1}}{q_i}=a_{i+1}+\frac{q_{i-1}}{q_i}$, то

$$\psi_i=\alpha_{i+1}+\frac{q_{i-1}}{q_i}=\frac{1}{\alpha_{i+2}}+\frac{q_{i+1}}{q_i}. \tag{10}$$

В силу доказанной нами леммы из двух отношений $\frac{q_{n+1}}{q_n}$ и $\frac{q_{n+2}}{q_{n+1}}$ по меньшей мере одно превосходит γ. Пусть для определённости $\frac{q_{n+1}}{q_n}>\gamma$. Так как функция $u+\frac{1}{u}$ возрастает при $u>1$, то в случае $\alpha_{n+2}\geqslant\frac{q_{n+1}}{q_n}$ мы имеем:

$$\psi_{n+1}=\alpha_{n+2}+\frac{q_n}{q_{n+1}}\geqslant\alpha_{n+2}+\frac{1}{\alpha_{n+2}}>\gamma+\frac{1}{\gamma}=\sqrt{5},$$

---

[1]) Разумеется, знаки равенства здесь невозможны ввиду иррациональности числа γ.

а в случае $\alpha_{n+2} < \frac{q_{n+1}}{q_n}$ в силу (10)

$$\psi_n = \frac{1}{\alpha_{n+2}} + \frac{q_{n+1}}{q_n} > \frac{1}{\frac{q_{n+1}}{q_n}} + \frac{q_{n+1}}{q_n} > \gamma + \frac{1}{\gamma} = \sqrt{5}.$$

Мы предположили для определённости $\frac{q_{n+1}}{q_n} > \gamma$. Но если бы было $\frac{q_{n+2}}{q_{n+1}} > \gamma$, то та же цепь рассуждений, с повышением только всех индексов на единицу, показала бы нам, очевидно, что либо $\psi_{n+2} > \sqrt{5}$, либо $\psi_{n+1} > \sqrt{5}$. Таким образом, первое утверждение теоремы 6 доказано.

Для доказательства второго утверждения рассмотрим число $\alpha = \gamma$; так как $\gamma = 1 + \frac{1}{\gamma}$, то, очевидно, $\alpha = [1;\ 1,\ 1,\ 1, \ldots]$, т. е. $a_n = 1$, $\alpha_n = \alpha$ для любого n; отсюда

$$\frac{p_0}{q_0} = \frac{1}{1}, \quad \frac{p_1}{q_1} = \frac{2}{1}, \quad \frac{p_2}{q_2} = \frac{3}{2},$$

так что $q_1 = p_0$, $q_2 = p_1$; опираясь на формулы $p_{n+1} = p_n + p_{n-1}$, $q_{n+1} = q_n + q_{n-1}$, мы полной индукцией немедленно устанавливаем, что для любого n

$$q_{n+1} = p_n,$$

и

$$\frac{q_{n+1}}{q_n} = \frac{p_n}{q_n} \to \alpha = \gamma \qquad (n \to \infty).$$

Поэтому, как бы мало ни было $\varepsilon > 0$, при достаточно большом n

$$\frac{q_{n+1}}{q_n} < \gamma + \varepsilon,$$

и, следовательно, в силу (10)

$$\psi_n < \frac{1}{\gamma} + \gamma + \varepsilon = \sqrt{5} + \varepsilon;$$

отсюда для всех достаточно больших n

$$\left|\gamma - \frac{p_n}{q_n}\right| > \frac{1}{(\sqrt{5} + \varepsilon)\, q_n^2}.$$

Таким образом, если $c < \frac{1}{\sqrt{5}}$, то среди подходящих дробей числа γ может быть лишь конечное число таких, для которых

$$\left|\gamma - \frac{p_n}{q_n}\right| < \frac{c}{q_n^2};$$

а так как среди дробей, не служащих подходящими дробями числа γ, в силу теоремы 3 вообще ни одна не может удовлетворять этому неравенству, то и второе утверждение теоремы 6 доказано.

§ 14. Диофантовы приближения

Мы уже видели, что тривиальный на первый взгляд переход от разности $\left|\alpha-\frac{p}{q}\right|$ к разности $|q\alpha-p|$ (служащей в качестве меры для оценки точности приближения) привёл нас как к более законченному решению ранее поставленных задач, так и к естественному возникновению новой проблематики. Однако его значение в этом последнем направлении нами ещё далеко не исчерпано. Принципиально наиболее важными и исторически наиболее значительными здесь оказались такие линии развития, которые выходят далеко за пределы не только теории цепных дробей, но и всей проблемы приближения действительных чисел рациональными дробями. К этим весьма широким выводам мы и должны теперь обратиться.

Когда мы искали такие целые числа q и p, для которых разность $q\alpha-p$ становится весьма малой по абсолютному значению (а именно так мы ставили задачу в первой половине этой главы), то можно, очевидно, сказать, что мы занимались приближённым решением в целых числах x, y уравнения

$$x\alpha-y=0, \tag{11}$$

где α было данным действительным числом; мы требовали при этом, чтобы x было положительным, и этим исключали тривиальное точное решение $x=y=0$. Если число α рационально, то уравнение (11) всегда имеет бесчисленное множество нетривиальных (т. е. отличных от раз навсегда исключаемого тривиального решения $x=y=0$) точных решений. Напротив, если α иррационально, то уравнение (11) не может иметь других точных решений, кроме тривиального. Поэтому здесь встаёт вопрос о приближённом его решении и о тех закономерностях, которые здесь имеют место. Этим вопросом мы и занимались до сих пор. Так, например, только что установленную нами теорему 6 с нашей новой точки зрения можно формулировать так, что *при иррациональном α уравнение* (11) *имеет бесчисленное множество таких приближённых решений $x>0$, y, для которых*

$$|x\alpha-y|<\frac{1}{\sqrt{5}\,x},$$

и что $\frac{1}{\sqrt{5}}$ *есть наименьшая положительная постоянная, могущая выступать в этой роли.*

Лежен Дирихле принадлежит заслуга создания замечательного своей простотой и мощностью метода, позволяющего изучать задачу приближённого решения уравнения (11) (и, как мы скоро увидим, много других аналогичных задач) без применения как цепных дробей, так и вообще какого бы то ни было специального аппарата.

Пусть мы хотим сделать:

$$|x\alpha - y| < \frac{1}{t} \qquad (x > 0), \tag{12}$$

где t — данное (большое) натуральное число. Сколь большим нам придётся для этого выбрать число x (а значит, и y)? Чтобы решить этот вопрос, заставим x пробегать ряд чисел $0, 1, 2, \ldots, t$ и для каждого из этих значений возьмём «дробную часть» произведения $x\alpha$

$$x\alpha - [x\alpha].$$

Таким образом, мы получим $t+1$ чисел $x\alpha - [x\alpha]$, удовлетворяющих, очевидно, неравенствам

$$0 \leqslant x\alpha - [x\alpha] < 1 \qquad (0 \leqslant x \leqslant t).$$

Если мы теперь разобьём отрезок $(0, 1)$ на t равных отрезков (длины $\frac{1}{t}$), причём к каждому из этих отрезков причислим его левый конец, но не будем причислять правого, то, очевидно, каждое из наших чисел $x\alpha - [x\alpha]$ будет принадлежать в точности одному из этих частных отрезков. Но чисел у нас $t+1$, а отрезков — только t; поэтому обязательно найдётся такой отрезок, который содержит два числа $x_1\alpha - [x_1\alpha]$ и $x_2\alpha - [x_2\alpha]$. Но тогда разность этих двух чисел будет меньше, чем длина содержащего их отрезка, т. е. меньше чем $\frac{1}{t}$. Допуская для определённости, что $x_1 < x_2$, и полагая $x_2 - x_1 = x$, $[x_2\alpha] - [x_1\alpha] = y$, мы поэтому будем иметь:

$$|x\alpha - y| < \frac{1}{t},$$

причём, очевидно, $0 < x \leqslant t$. Мы приходим, таким образом, к следующему важному предложению, принадлежащему Дирихле:

Теорема 7. *Пусть α — любое действительное число и t — любое натуральное число; тогда существуют такие целые числа x и y, что*

$$|x\alpha - y| < \frac{1}{t} \qquad (0 < x \leqslant t). \tag{13}$$

Таким образом, неравенствам (12) всегда можно удовлетворить, выбирая x не бóльшим, чем данное число t. Из неравенств (13), очевидно, вытекает неравенство

$$|x\alpha - y| < \frac{1}{x},$$

существование сколь угодно больших решений которого нам хорошо известно из теории цепных дробей; теперь мы доказали его методом Дирихле без всякого алгорифма. Впрочем, теорема 7 очень легко доказывается и с помощью цепных дробей:

пусть $\frac{p_n}{q_n}$ — подходящие дроби числа α; выберем (что всегда возможно) n так, чтобы $q_n \leqslant t < q_{n+1}$; тогда, как известно,

$$|q_n\alpha - p_n| < \frac{1}{q_{n+1}} < \frac{1}{t} \qquad (q_n \leqslant t),$$

что и доказывает теорему 7. Однако главное преимущество метода Дирихле состоит не в его элементарности (хотя и этот момент, конечно, достаточно важен). Его мощность встаёт в полный рост тогда, когда мы от простейшего уравнения (11) переходим к более сложным и общим задачам.

Дирихле обратил внимание на то, что задача, которую мы только что решили для уравнения (11), может быть в точности так же поставлена и для более общего уравнения

$$x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n - y = 0,$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — данные действительные числа, а $x_1, \ldots, x_n, y$ — целочисленные переменные, причём тривиальное решение $x_1 = x_2 = \ldots = x_n = y = 0$ также, разумеется, раз навсегда исключается. Можно ли надлежащим (нетривиальным) выбором целых x_i, y сделать абсолютную величину разности

$$\sum_{i=1}^{n} x_i\alpha_i - y$$

сколь угодно малой и, если можно, то сколь большими придётся для этого выбирать числа $|x_i|$ (а следовательно, и $|y|$)? Было бы безнадёжно пытаться использовать для решения этой задачи аппарат цепных дробей: как показала история развития этой области математики, не существует (и, повидимому, не может существовать) такого удовлетворительного во всех отношениях алгорифма для совместного арифметического исследования нескольких иррациональностей $\alpha_1, \alpha_2, \ldots, \alpha_n$, какой мы имеем для случая одной иррациональности α в лице цепных дробей. Напротив, метод Дирихле, как мы сейчас покажем, применяется к новой, общей задаче с такой же лёгкостью и приводит к столь же простому её решению, как и в случае рассмотренной нами выше простейшей задачи.

Заставим переменные $x_1, x_2, \ldots, x_n$ пробегать независимо друг от друга ряд чисел $0, 1, \ldots, t$ (где t — любое данное натуральное число). Очевидно, мы получим всего $(t+1)^n$ систем значений $(x_1, x_2, \ldots, x_n)$, а следовательно, столько же значений суммы $\sum_{i=1}^{n} x_i\alpha_i$ и столько же дробных частей

$$\sum_{i=1}^{n} x_i\alpha_i - \left[\sum_{i=1}^{n} x_i\alpha_i\right] \tag{14}$$

(среди этих дробных частей могут быть и равные между собою; это замечание, впрочем, относится и к рассмотренному выше простейшему случаю; там, как и тут, оно ничем не мешает строгости доказательства).

Разобьём теперь отрезок (0, 1) на t^n равных отрезков (длины $\frac{1}{t^n}$), причём снова будем считать левый конец принадлежащим, а правый — не принадлежащим каждому такому частичному отрезку. Снова каждая из наших дробных частей (14) принадлежит в точности одному из частичных отрезков, и снова число $(t+1)^n$ дробных частей больше чем число t^n отрезков. Поэтому снова найдётся отрезок, содержащий по меньшей мере две из дробных частей (14). Пусть эти две дробные части получены для значений переменных

$$x_1', x_2', \ldots, x_n' \quad \text{и} \quad x_1'', x_2'', \ldots, x_n''.$$

Полагая

$$x_i'' - x_i' = x_i \ (1 \leqslant i \leqslant n), \quad \left[\sum_{i=1}^{n} x_i'' \alpha_i\right] - \left[\sum_{i=1}^{n} x_i' \alpha_i\right] = y,$$

мы, как и ранее, получаем:

$$\left|\sum_{i=1}^{n} x_i \alpha_i - y\right| < \frac{1}{t^n},$$

причём $|x_i| \leqslant t$ и, разумеется, не все x_i равны нулю (что удобно выражать неравенством $\sum_{i=1}^{n} x_i^2 > 0$). Таким образом, мы приходим к следующей общей теореме, также установленной Дирихле:

Теорема 8. *Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — любые действительные числа и t — любое натуральное число; тогда существуют такие целые числа $x_1, x_2, \ldots, x_n, y$, что*

$$\left|\sum_{i=1}^{n} x_i \alpha_i - y\right| < \frac{1}{t^n}, \quad |x_i| \leqslant t \ (1 \leqslant i \leqslant n), \quad \sum_{i=1}^{n} x_i^2 > 0.$$

Если обозначить через x наибольшее из чисел $|x_1|, |x_2|, \ldots, |x_n|$, то из теоремы 8, очевидно, вытекает

Следствие. *В условиях теоремы 8 существует бесчисленное множество таких систем значений $x_1, x_2, \ldots, x_n, y$, что*

$$\left|\sum_{i=1}^{n} x_i \alpha_i - y\right| < \frac{1}{x^n}.$$

Это важное неравенство, обобщающее хорошо известное из теории цепных дробей неравенство

$$|q\alpha - p| < \frac{1}{q},$$

также не могло бы быть установлено известными алгорифмическими методами и является замечательным достижением метода Дирихле.

Вступив на этот путь обобщений, наука скоро увидела здесь перед собой неисчерпаемое поле для исследований. От общего линейного однородного уравнения, которым мы только что занимались, представилось естественным перейти, с одной стороны, к системам таких уравнений, а с другой, — к неоднородным уравнениям. Можно, конечно, вообще не ограничиваться одними только линейными уравнениями, а перейти к алгебраическим уравнениям высших степеней, а затем и к некоторым трансцендентным уравнениям. Так создавалось учение о приближённом решении уравнений в целых числах, которое, по предложению Минковского, принято теперь называть теорией диофантовых приближений — наименование очень удачное, так как диофантовыми уравнениями называют уже давно уравнения, в которых неизвестные могут принимать только целые значения. Основоположниками этого учения были Дирихле, Чебышев, Кронекер и Минковский. В частности, Минковским был создан в этой области глубокий и очень сильный метод, состоящий в систематическом применении к задачам теории чисел геометрических закономерностей (так называемая «геометрия чисел»).

Простейшая из неоднородных линейных задач этой области состоит, очевидно, в исследовании законов приближённого решения уравнения

$$x\alpha - y - \beta = 0, \tag{15}$$

где α и β — данные действительные числа, а x и y — целочисленные неизвестные. Эту задачу впервые поставил и далеко исследовал великий русский учёный П. Л. Чебышев. Если предположить, что $0 < \beta < 1$ (что, очевидно, не ограничивает общности постановки задачи), то $y = [x\alpha]$, и задача Чебышева состоит в исследовании таких целых значений x, для которых дробная часть произведения $x\alpha$ близка к данному заранее числу β, подобно тому как прежде мы искали значения x, для которых эта дробная часть близка к нулю. Уже самая возможность при любом $\varepsilon > 0$ подобрать целые x, y так, чтобы

$$|x\alpha - y - \beta| < \varepsilon \tag{16}$$

(т. е. возможность приближённого решения уравнения (15) с любой степенью точности), здесь совсем не ясна с самого начала. Если, например, число $\alpha = \frac{a}{b}$ рационально, то ясно, что $x\alpha - y$ при любых целых x, y также будет рациональной дробью со знаменателем b; поэтому, если β отстоит на расстояние δ от ближайшей к нему дроби со знаменателем b, то неравенство

$$|x\alpha - y - \beta| < \delta$$

невыполнимо ни при каких целых x и y.

Тем более замечательно, что *если число* α *иррационально, то, каково бы ни было* β, *неравенство* (16) *при любом* $\varepsilon > 0$ *может быть реализовано надлежаще выбранными целыми* x, y. Проще всего это может быть доказано следующим рассуждением. Из теории цепных дробей мы знаем, что для иррационального α целые числа q и p могут быть выбраны так, что

$$0 < q\alpha - p < \varepsilon;$$

положим для краткости $q\alpha - p = \lambda$ и рассмотрим последовательность чисел

$$0,\ \lambda,\ 2\lambda,\ \ldots,\ k\lambda,\ \ldots$$

Очевидно, найдётся такое $k \geqslant 0$, что

$$k\lambda \leqslant \beta < (k+1)\lambda,$$

откуда

$$|k\lambda - \beta| = |kq\alpha - kp - \beta| < \lambda < \varepsilon,$$

так что, полагая $x = kq$, $y = kp$, мы действительно реализуем неравенство (16).

До сих пор мы занимались только вопросом о возможности приближённого решения уравнения (15) с любой наперёд заданной степенью точности, не спрашивая себя о том, как велики будут числа x и y, потребные для этой цели. Можно, однако, пойти в этом направлении гораздо дальше и установить для неоднородной задачи законы, вполне аналогичные тем, какие мы нашли в предыдущем разделе для однородной задачи. Мы ограничимся доказательством теоремы, принадлежащей Чебышеву и составляющей важнейший результат его замечательного исследования.

Теорема 9. *Если* α *— иррациональное,* β *— любое действительное число, то существует бесчисленное множество целых значений чисел* x *и* y, *для которых*

$$|x\alpha - y - \beta| < \frac{3}{|x|}.$$

Доказательство. Пусть $\frac{p}{q}$ — подходящая дробь числа α, так что

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2};$$

обозначим через r ближайшее к произведению $q\beta$ целое число, так что

$$|q\beta - r| \leqslant \frac{1}{2}, \quad \left|\beta - \frac{r}{q}\right| \leqslant \frac{1}{2q}. \tag{17}$$

Как мы знаем из главы II, сравнению

$$px \equiv r \pmod{q}$$

можно удовлетворить числом x, лежащим в любом наперёд заданном отрезке длины q натурального ряда. Пусть поэтому

$$px \equiv r \pmod{q}, \quad \frac{q}{2} \leqslant x < \frac{3q}{2},$$

так что

$$q > \frac{2}{3} x, \tag{18}$$

и пусть

$$px - r = qy. \tag{19}$$

Тогда в силу (17), (18) и (19)

$$|x\alpha - y - \beta| = \left| x\left(\alpha - \frac{p}{q}\right) - \left(\beta - \frac{r}{q}\right) + \frac{px - qy - r}{q} \right| =$$
$$= \left| x\left(\alpha - \frac{p}{q}\right) - \left(\beta - \frac{r}{q}\right) \right| < \frac{x}{q^2} + \frac{1}{2q} < \frac{3}{x};$$

так как при этом в силу $x \geqslant \frac{1}{2} q$ числа x и y могут быть выбраны сколь угодно большими, то теорема 9 доказана.

Постоянная 3 в правой части доказанного неравенства может быть значительно снижена. Как доказал Минковский, в случае, когда уравнение (15) не может быть точно решено в целых числах, наилучшее значение этой постоянной есть $\frac{1}{4}$.

ГЛАВА VI

АЛГЕБРАИЧЕСКИЕ И ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА

§ 15. Теорема Лиувилля и первое появление трансцендентных чисел

Всякое рациональное число $\frac{a}{b}$ есть корень уравнения первой степени с целыми коэффициентами

$$bx - a = 0,$$

и обратно, корень всякого такого уравнения есть некоторое рациональное число. Множество рациональных чисел есть, таким образом, множество корней всех уравнений первой степени с целыми коэффициентами. Став на эту точку зрения, мы, естественно, будем склонны считать, что простейшими иррациональными числами нужно будет признать те, которые удовлетворяют квадратным уравнениям

$$ax^2 + bx + c = 0 \tag{1}$$

с целыми коэффициентами a, b, c. И действительно, первые иррациональности, с которыми мы встречаемся уже на школьной скамье, — это квадратные корни из целых или, общéе, рациональных чисел; но всякое такое число

$$\alpha = \sqrt{\frac{p}{q}} \tag{2}$$

есть корень квадратного уравнения

$$qx^2 - p = 0,$$

представляющего собой разновидность уравнения (1). Как известно, и обратно — корни любого уравнения (1) с целыми a, b, c рационально выражаются через иррациональности типа (2). Дальше мы в школьном курсе встречаемся с корнями третьей, четвёртой и т. д. степеней из рациональных чисел; такие иррациональности являются, аналогично предшествующему, корнями уравнений третьей, четвёртой и т. д. степеней с целыми коэффициентами.

Обобщая эти замечания, мы естественно приходим к общему рассмотрению таких действительных чисел, которые являются корнями какого-либо алгебраического уравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \qquad (3)$$

с целыми a_0, a_1, ... , a_n. Такие числа называют *алгебраическими*. Если число α служит корнем уравнения (3), но не удовлетворяет никакому уравнению того же типа степени $< n$, то α называют *алгебраическим числом порядка n* (или *степени n*). Таким образом, рациональные числа могут быть определены как алгебраические числа первой степени (или первого порядка), $\sqrt{2}$ есть алгебраическое число второй степени и т. д.

Первый и основной вопрос, встающий после введения этого нового понятия, очевидно, гласит: существуют ли такие действительные числа, которые не являются алгебраическими, т. е. не удовлетворяют никакому уравнению типа (3) с целыми коэффициентами? Первый ответ на этот вопрос, а также и первые примеры таких неалгебраических чисел были даны Лиувиллем около середины XIX столетия. Путь Лиувилля был следующий: сначала он показал, что для алгебраических чисел при их приближении рациональными дробями необходимо должны наблюдаться некоторые специфические закономерности; потом он легко построил примеры чисел, приближение которых этим закономерностям не подчиняется и которые, следовательно, не могут быть алгебраическими.

Все неалгебраические числа называются *трансцендентными* (т. е. «выходящими за пределы»). Трансцендентные числа Лиувилля, к построению которых мы сейчас перейдём, были исторически первым примером этого рода чисел.

Пусть α — алгебраическое число степени n, удовлетворяющее уравнению (3) (и не удовлетворяющее никакому уравнению низшей степени). Будем для краткости обозначать через $f(x)$ левую часть уравнения (3), так что $f(\alpha) = 0$. Если бы многочлен $f(x)$ имел рациональный корень $\frac{a}{b}$, то $f(x)$ делилось бы по теореме Безу на $x - \frac{a}{b}$, и мы имели бы

$$f(x) = (x - \tfrac{a}{b}) f_1(x),$$

где $f_1(x)$ — многочлен степени $n - 1$ с рациональными коэффициентами. Так как $f(\alpha) = 0$ и $\alpha - \frac{a}{b} \neq 0$, то мы имели бы: $f_1(\alpha) = 0$; если обозначить через g общий знаменатель коэффициентов многочлена $f_1(x)$, то $gf_1(x)$ есть многочлен степени $n - 1$ с целыми коэффициентами и $g f_1(\alpha) = 0$, что невозможно, так как α есть, по предположению, алгебраическое число степени n. Полученное

противоречие показывает, что многочлен $f(x)$ не может иметь рациональных корней.

По теореме Безу из $f(\alpha)=0$ следует, что тождественно

$$f(x)=(x-\alpha)\varphi(x),$$

где $\varphi(x)$ — многочлен степени $n-1$. Полагая $x=\frac{p}{q}$, мы находим:

$$f\left(\frac{p}{q}\right)=\left(\frac{p}{q}-\alpha\right)\varphi\left(\frac{p}{q}\right). \tag{4}$$

Допустим теперь, что $\frac{p}{q}$ есть рациональная дробь, лежащая в отрезке $(\alpha-1,\ \alpha+1)$, и обозначим через β наибольшее значение функции $|\varphi(x)|$ в этом отрезке, так что, в частности,

$$\left|\varphi\left(\frac{p}{q}\right)\right|\leqslant\beta. \tag{5}$$

Так как по доказанному

$$\left|f\left(\frac{p}{q}\right)\right|=\left|\frac{a_0p^n+a_1p^{n-1}q+\ldots+a_nq^n}{q^n}\right|>0,$$

то $\left|f\left(\frac{p}{q}\right)\right|\geqslant\frac{1}{q^n}$, и соотношение (4) в силу неравенства (5) даёт:

$$\left|\alpha-\frac{p}{q}\right|\geqslant\frac{1}{\beta q^n}.$$

Так обстоит дело для любой рациональной дроби $\frac{p}{q}$, принадлежащей отрезку $(\alpha-1,\ \alpha+1)$. Но если $\frac{p}{q}$ лежит вне этого отрезка, то

$$\left|\alpha-\frac{p}{q}\right|\geqslant 1\geqslant\frac{1}{q^n};$$

поэтому, если λ означает меньшее из чисел 1 и $\frac{1}{\beta}$, то уже для л ю б о й рациональной дроби $\frac{p}{q}$

$$\left|\alpha-\frac{p}{q}\right|\geqslant\frac{\lambda}{q^n}. \tag{6}$$

Мы приходим, таким образом, к следующему общему предложению, составляющему основу метода Лиувилля:

Т е о р е м а Л и у в и л л я. *Для всякого алгебраического числа α степени n существует такое положительное число λ, что, какова бы ни была рациональная дробь $\frac{p}{q}$, имеет место неравенство* (6).

Вглядимся в смысл этого предложения. Мы знаем, что для любого иррационального числа α существует бесчисленное множество

таких рациональных дробей $\frac{p}{q}$, что

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2};$$

это можно рассматривать как некий универсальный (т. е. реализующийся для всякого иррационального α) закон приближения. Однако могут существовать и такие α, для которых имеют место гораздо более сильные приближения. Мы скоро увидим, что в этом отношении не может быть никакого предела, что существуют иррациональности, которые аппроксимируются рациональными дробями лучше, чем по любому наперёд заданному закону. Теорема Лиувилля показывает, что для алгебраических иррациональностей приближение рациональными дробями уже не может быть сколь угодно тесным; его близость ограничивается некоторым определённым законом (зависящим, кстати сказать, от степени данного алгебраического числа). Так, например, для квадратической иррациональности α ($n = 2$) всегда существует такое $\lambda > 0$, что при любых p и q

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{\lambda}{q^2},$$

т. е. квадратические иррациональности (например, $\sqrt{2}$, $\sqrt{5}$ и т. д.) никогда не могут быть аппроксимируемы лучше, чем по «универсальному» закону.

Таким образом, если нам удастся построить такое число, которое при любом n допускает приближения рациональными дробями, более сильные, чем допускаемые теоремой Лиувилля, то это число по необходимости будет трансцендентным. И вот оказывается, что такого рода числа (так называемые «трансцендентные числа Лиувилля») могут быть построены с большою лёгкостью; с этой целью может быть использован любой из аппаратов, служащих для приближённого представления чисел рациональными дробями; но можно конструировать их и не опираясь ни на какой специальный аппарат.

Возьмём, например, аппарат цепных дробей. Положим $a_0 = 0$, а дальнейшие элементы конструируемой дроби будем определять по следующему рекуррентному правилу: если $a_0, a_1, \ldots, a_n$ уже определены (а следовательно, определена и подходящая дробь $\frac{p_n}{q_n}$), то положим: $a_{n+1} = q_n^n$. Построенная таким образом цепная дробь $[a_0; a_1, a_2, \ldots, a_n, \ldots]$ представляет, как мы знаем, некоторое иррациональное число α; покажем, что это число — трансцендентное.

В самом деле, мы знаем, что для любого k

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}} = \frac{1}{q_k (q_k a_{k+1} + q_{k-1})} < \frac{1}{q_k^2 a_{k+1}};$$

так как $a_{k+1} = q_k^k$, то отсюда

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^{2+k}}.$$

Если теперь $\lambda > 0$ и натуральное число n заданы произвольно, и если число $k \geqslant n$ настолько велико, что $\frac{1}{q_k^2} < \lambda$, то

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^{k+2}} < \frac{\lambda}{q_k^k} \leqslant \frac{\lambda}{q_k^n}.$$

Поэтому число α согласно теореме Лиувилля не может быть алгебраическим числом степени n; а так как n произвольно, то число α вообще не может быть алгебраическим.

Теперь проведём построение примера трансцендентного числа без всякого алгорифма. Начнём с любой несократимой дроби $\frac{p_1}{q_1}$. Окружим её отрезком

$$\Delta_1 = \left(\frac{p_1}{q_1} - \frac{1}{q_1},\ \frac{p_1}{q_1} + \frac{1}{q_1}\right).$$

В отрезке Δ_1 выберем другую несократимую дробь $\frac{p_2}{q_2}$, так чтобы $q_2 > q_1$, и окружим её отрезком

$$\Delta_2 = \left(\frac{p_2}{q_2} - \frac{1}{q_2^2},\ \frac{p_2}{q_2} + \frac{1}{q_2^2}\right).$$

Вообще, если отрезок Δ_{n-1} уже построен, то мы выбираем в нём произвольно несократимую дробь $\frac{p_n}{q_n}$, так чтобы $q_n > q_{n-1}$, и окружаем её отрезком

$$\Delta_n = \left(\frac{p_n}{q_n} - \frac{1}{q_n^n},\ \frac{p_n}{q_n} + \frac{1}{q_n^n}\right).$$

Этот процесс мы можем продолжать безгранично. Покажем, что отрезок Δ_n целиком лежит внутри отрезка Δ_{n-1} ($n \geqslant 2$). В самом деле, если бы, например, правый конец Δ_n лежал правее правого конца Δ_{n-1} (или совпадал с ним), то это означало бы:

$$\frac{p_n}{q_n} < \frac{p_{n-1}}{q_{n-1}} + \frac{1}{q_{n-1}^{n-1}} \leqslant \frac{p_n}{q_n} + \frac{1}{q_n^n},$$

откуда

$$0 < \frac{p_{n-1}}{q_{n-1}} + \frac{1}{q_{n-1}^{n-1}} - \frac{p_n}{q_n} \leqslant \frac{1}{q_n^n}.$$

Но средняя часть этих неравенств есть положительная дробь со знаменателем $q_{n-1}^{n-1} q_n$; значит, она не меньше чем $\frac{1}{q_{n-1}^{n-1} q_n}$, и получаем:

$$\frac{1}{q_{n-1}^{n-1} q_n} \leqslant \frac{1}{q_n^n},$$

откуда $q_n \leqslant q_{n-1}$, что неверно.

Итак, Δ_n целиком содержится внутри Δ_{n-1}; а так как при $n \to \infty$ длина отрезка Δ_n стремится к нулю, то существует единственное число α, принадлежащее всем отрезкам Δ_n ($n = 1, 2, \ldots$).

Пусть теперь снова произвольно заданы $\lambda > 0$ и натуральное число n; пусть $k > n$ и столь велико, что $\frac{1}{q_k} < \lambda$; тогда, так как α принадлежит отрезку Δ_k, мы имеем:

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^k} = \frac{1}{q_k} \cdot \frac{1}{q_k^{k-1}} < \frac{\lambda}{q_k^n}.$$

Так как n и $\lambda > 0$ произвольны, то в силу теоремы Лиувилля число α трансцендентно.

§ 16. Метод Кантора

Спустя 20—25 лет после работ Лиувилля стали появляться исследования Георга Кантора, положившие начало новой важнейшей ветви математической науки — теории множеств. Одним из первых плодов этих исследований явилось новое, глубоко оригинальное доказательство существования трансцендентных чисел. Это был образец такого математического рассуждения, какое до тех пор ещё никогда не применялось в науке, а в дальнейшем послужило прототипом для целого ряда других плодотворных конструкций.

Кантор впервые обратил серьёзное внимание на тот факт, что все алгебраические числа можно пересчитать. Что это значит? Это значит, как и обычно, что можно каждому алгебраическому числу придать определённый, одному ему приписанный номер. Понятно, что никакого конечного числа номеров для этой цели нехватит, потому что алгебраических чисел — бесконечное множество (к ним принадлежат все рациональные и, в частности, все натуральные числа). Но в нашем распоряжении находится безграничный ряд номеров — все натуральные числа. И вот оказывается, что с помощью этого бесконечного ряда натуральных номеров можно перенумеровать все алгебраические числа, подобно тому как с помощью первых десяти натуральных чисел можно перенумеровать все пальцы рук. Но не тривиально ли это? Натуральных чисел бесконечно много, а имея неограниченный запас номеров, не можем ли мы с их помощью перенумеровать предметы любого множества? Кантор показал (и это, быть может, самый блестящий из его первых результатов), что это не так: множество C всех действительных чисел не может быть перенумеровано даже с помощью всего бесконечного ряда натуральных чисел. Отсюда уже прямо следует существование трансцендентных чисел: если бы их не было, то множество C совпадало бы со множеством A всех алгебраических чисел и, следовательно, могло бы быть перенумеровано.

Посмотрим теперь, как можно перенумеровать все алгебраические числа. Каждое алгебраическое число есть корень некоторого алгебраического уравнения вида (3), причём $a_0, a_1, \ldots, a_n$ — целые

числа и $a_0 \neq 0$. Назовём «высотою» этого уравнения положительное целое число

$$h = n + |a_0| + |a_1| + \ldots + |a_n|.$$

Если высота h уравнения дана, то и степень его и абсолютные значения коэффициентов ограничены; поэтому может существовать лишь конечное число уравнений вида (3) с данной высотой h. Так, совокупность уравнений высоты 3 исчерпывается, очевидно, уравнениями

$$x^2 = 0, \quad -x^2 = 0, \quad x + 1 = 0, \quad x - 1 = 0,$$
$$-x + 1 = 0, \quad -x - 1 = 0, \quad 2x = 0, \quad -2x = 0.$$

Это обстоятельство позволяет нам в первую очередь перенумеровать все уравнения типа (3). Наименьшая возможная высота уравнения есть, очевидно, $h = 2$, и уравнений с такой высотой только два: $x = 0$ и $-x = 0$. Эти два уравнения мы снабжаем соответственно номерами 1 и 2. Затем мы переходим к выписанным выше восьми уравнениям высоты 3 и последовательно придаём им следующие номера: 3, 4, 5, 6, 7, 8, 9, 10. Потом мы переходим к уравнениям высоты 4 и последовательно нумеруем их числами 11, 12, ... Так как каждой высоте соответствует лишь конечная группа уравнений, то при безграничном продолжении описанного процесса действительно каждое уравнение типа (3) рано или поздно получит свой, ему одному приписанный номер. Таким образом, множество всех уравнений типа (3) может быть перенумеровано.

А теперь перейдём к нумерации (действительных) алгебраических чисел. Основою этой нумерации будет служить то, что в силу основной теоремы алгебры уравнение вида (3) может иметь лишь конечное (не более n) число корней. Возьмём уравнение № 1, и пусть оно имеет n_1 различных между собою действительных корней; обозначим эти корни через $\alpha_1, \alpha_2, \ldots, \alpha_{n_1}$. Перейдём к уравнению № 2; пусть оно имеет n_2 действительных корней, отличных друг от друга и от корней уравнения № 1; обозначим эти корни через $\alpha_{n_1+1}, \alpha_{n_1+2}, \ldots$ $\ldots, \alpha_{n_1+n_2}$. Далее, действительные корни уравнения № 3, отличные друг от друга и от корней уравнений № 1 и № 2, обозначим через

$$\alpha_{n_1+n_2+1}, \quad \alpha_{n_1+n_2+2}, \quad \ldots, \quad \alpha_{n_1+n_2+n_3},$$

если n_3 — число таких корней. Будем продолжать этот процесс безгранично. Мы получим ряд чисел

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots, \tag{7}$$

в котором каждое число, удовлетворяющее какому-либо уравнению типа (3), встретится один и только один раз. Таким образом, этот ряд представляет собою не что иное, как перенумерованное множество всех алгебраических чисел.

После того как такая нумерация произведена, построение примеров трансцендентных чисел не представляет уже никаких затруднений. Пусть цепная дробь, представляющая число α_k, имеет вид

$$\alpha_k = [a_0^{(k)};\ a_1^{(k)},\ a_2^{(k)},\ \ldots,\ a_n^{(k)},\ \ldots];$$

при этом мы условимся в случае, если α_k есть рациональное число и, следовательно, наша цепная дробь имеет последний элемент $a_n^{(k)}$, писать (только на этот раз!) $a_{n+1}^{(k)} = a_{n+2}^{(k)} = \ldots = 0$ (чтобы иметь возможность всякое действительное число представить б е с к о н е ч н о й цепной дробью).

Положим теперь для любого $k > 0$

$$b_k = a_k^{(k)} + 1.$$

Тогда цепная дробь

$$[0;\ b_1,\ b_2,\ \ldots,\ b_n,\ \ldots]$$

имеет все элементы, начиная с b_1, положительными и, следовательно, представляет некоторое действительное число β. Докажем, что это число — трансцендентное. В самом деле, так как ряд (7) содержит все алгебраические числа, то если бы число β было алгебраическим, оно должно было бы совпадать с одним из чисел α_k этого ряда; но в силу единственности представления чисел цепными дробями из $\beta = \alpha_k$ следует $b_n = a_n^{(k)}$ при любом $n \geqslant 0$ и, значит, в частности $b_k = a_k^{(k)}$, что противоречит определению числа b_k. Таким образом, трансцендентность числа β доказана.

Ясно, что мы можем при построении нашего трансцендентного числа как угодно варьировать определение чисел b_k, лишь бы было $b_k > 0$ и $b_k \neq a_k^{(k)}$. Это показывает, что метод Кантора позволяет легко построить сколько угодно трансцендентных чисел.

§ 17. Арифметическая природа классических постоянных

Мы видели во всех случаях, что построение действительных чисел с заранее заданными чертами их арифметической природы не представляет значительных затруднений: мы можем построить сколько угодно примеров чисел, заведомо иррациональных или заведомо трансцендентных, чисел, очень хорошо или, напротив, не слишком хорошо аппроксимируемых рациональными дробями, и т. д. Но несравненно более трудные задачи встают, когда мы хотим определить арифметические черты числа, появившегося в нашей научной практике под влиянием мотивов совсем не арифметического характера, пришедшего в арифметику, так сказать, извне. Будет ли число π, определяемое в геометрии как отношение длины окружности

к диаметру, рациональным или иррациональным, — об этом нам его определение не говорит ничего. Будет ли число e, определяемое в анализе как

$$e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$$

или как

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} + \ldots, \tag{8}$$

алгебраическим или трансцендентным и насколько хорошо оно аппроксимируется рациональными дробями, — всего этого непосредственно из его определений узнать не удаётся. А между тем, числа e и π играют во всей математике настолько фундаментальную роль, что нам трудно примириться с нашим полным незнанием их арифметических черт. Поэтому понятно, что изучение арифметической природы этих, а также других «классических постоянных» давно уже привлекало к себе внимание учёных; трудность же задачи, как всегда бывает в науке, только ещё более стимулировала энергию исследователей. И в наше время, хотя многие из задач этой области остаются и до сих пор нерешёнными, наука всё же с полным правом гордится замечательными достижениями в указанном направлении, — достижениями, стоившими напряжённых усилий сильнейшим умам, в особенности последнего столетия.

Сравнительно рано стало известным, что числа e и π иррациональны. Для числа e доказательство его иррациональности настолько просто, что мы можем привести его здесь; исходной точкой для нас будет при этом представление числа как суммы бесконечного ряда (8).

Если бы число e было рациональным, $e = \frac{a}{b}$, то число $b!e$ было бы целым; но ряд (8) даёт:

$$b!e = b! + \frac{b!}{1!} + \frac{b!}{2!} + \ldots + \frac{b!}{b!} + \\ + \frac{b!}{(b+1)!} + \frac{b!}{(b+2)!} + \ldots$$

В правой части все слагаемые первой строки — целые числа; а так как и левая часть есть в силу нашего предположения целое число, то целым числом должна быть и сумма слагаемых второй строки, т. е. величина

$$\alpha = \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \ldots;$$

но эта сумма положительна и в то же время, очевидно, меньше чем

$$\frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \ldots = \frac{1}{b} \leqslant 1;$$

следовательно, $0 < \alpha < 1$, и α не может быть целым числом, что и доказывает иррациональность числа e.

Доказательство иррациональности числа π значительно сложнее: для π мы не знаем уже столь простого и арифметически обозримого изображающего аппарата, каким служит ряд (8) для числа e. Исторически иррациональность числа π была впервые обнаружена, когда удалось найти разложение числа $\frac{\pi}{4}$ в цепную дробь; так как эта дробь оказалась бесконечной, то число $\frac{\pi}{4}$ — а следовательно, и π — иррационально.

Однако несравненно труднее было решить вопрос о том, является ли каждое из чисел e и π алгебраическим или трансцендентным. Трансцендентность числа e была впервые доказана Эрмитом в 1873 г. сложным аналитическим методом, основанным на рассмотрении некоторых определённых интегралов с бесконечными пределами. Ввиду той фундаментальной роли, которую играет число e в дифференциальном и интегральном исчислениях, привлечение интегралов к решению вопроса об арифметической природе этого числа отнюдь нельзя считать искусственным. Девять лет спустя Линдеман, развивая далее метод Эрмита, доказал трансцендентность числа π. Подход к этому числу методом Эрмита мог бы показаться странным, так как числа e и π по своему первоначальному определению ничем друг с другом не связаны; они для арифметики как бы пришельцы из разных стран. Однако замечательное, играющее выдающуюся роль в анализе соотношение $e^{\pi i} = -1$ тесно связывает их между собою и позволяет в принципе любой метод, созданный для изучения одного из них, применить и к другому; этой связью и воспользовался Линдеман в своих исследованиях.

После того как таким образом была установлена трансцендентность двух важнейших классических постоянных, в течение долгого времени в этой области не удавалось создать ничего нового. Насколько трудна и бедна сколько-нибудь общими методами эта проблематика, можно видеть из того, что мы до сих пор ничего не знаем об арифметической природе таких чисел, как $e + \pi$, $e - \pi$ или $e\pi$; не известно даже, будут ли они иррациональными. Гильберт в 1907 г. значительно упростил доказательства Эрмита и Линдемана для чисел e и π; Гурвицу удалось найти доказательства, вообще свободные от интегралов (но существенно пользующиеся дифференциальным исчислением). Но все эти исследования, чрезвычайно глубокие и в то же время изящные, всё же не были методологически сильнее прежних — не позволяли получить новых результатов.

На международном математическом конгрессе 1900 г. Гильберт в своём знаменитом докладе об актуальных математических проблемах современности обратил внимание на то, что мы, успешно справившись с такими со стороны пришедшими в арифметику числами,

как e и π, в то же время до сих пор ничего не знаем об арифметической природе некоторых чисел, так сказать, внутриарифметического происхождения. В качестве примера он указал на число $2^{\sqrt{2}}$ и вообще на числа вида α^β, где α и β — алгебраические числа, причём α отлично от 0 и 1, а β — иррационально (в частности, таким числом является e^π, так как из $e^{\pi i} = -1 = i^2$ следует $e^\pi = i^{-2i}$). Эта задача Гильберта получила весьма широкую известность; однако в течение тридцати лет в этом направлении не было получено никаких результатов, и казалось, что и подхода к этому кругу проблем никакого не видно. Но в 30-х годах нашего столетия тогда ещё очень молодой советский учёный А. О. Гельфонд открыл весьма сильный общий метод, основанный на теории функций комплексного переменного и позволивший решить задачу Гильберта сначала для некоторых классов, а затем (в 1936 г.) и для всех указанных Гильбертом чисел: Гельфонд доказал, что все эти числа без исключения трансцендентны. Замечательные методы, созданные советским учёным, были затем им самим постепенно усовершенствованы и в настоящее время дают возможность устанавливать трансцендентность весьма широких классов чисел.

Литература

1. Полное собрание сочинений П. Л. Чебышева, т. I, Теория чисел. Издательство АН СССР, М.—Л., 1944.

В этом томе собраны все классические произведения П. Л. Чебышева по теории чисел, а именно: его «Теория сравнений», представляющая превосходный, ясно и доступно написанный курс теории чисел, исследования закона распределения простых чисел в натуральном ряде и др.

2. Виноградов И. М., Основы теории чисел, издание пятое, переработанное. Гостехиздат, М. — Л., 1949.

Сжато, но просто и отчётливо написанный курс теории чисел, содержащий значительное количество оригинальных задач и вопросов с решениями.

3. Арнольд И. В., Теория чисел, Пособие для пединститутов, Учпедгиз, М., 1939.

Хороший учебник теории чисел, включающий, помимо основного элементарного курса, много сведений из других отделов современной теории чисел, частично без доказательств. В конце книги даны упражнения по теории чисел.

4. Диксон Л. Е., Введение в теорию чисел, Обработанный перевод с англ. Вып. I, Тбилиси, 1941.

Книга ценна собранием задач, особенно на неопределённые уравнения высших степеней, снабжённых в русском издании подробными решениями.

5. Делоне Б. Н., Петербургская школа теории чисел. Издательство АН СССР, М. — Л., 1947.

Книга в хронологическом порядке знакомит с творчеством крупнейших русских учёных, работавших по теории чисел: П. Л. Чебышева, А. Н. Коркина, Е. И. Золотарёва, А. А. Маркова, Г. Ф. Вороного и И. М. Виноградова.

6. Шнирельман Л. Г., Простые числа, Гостехиздат. М. — Л., 1940.

Небольшая (60 стр. малого формата), но весьма содержательная брошюра, представляющая введение в теорию чисел. В неё входят: основы теории сравнений, основы арифметики комплексных чисел, некоторые результаты Чебышева с упрощёнными доказательствами и др.; за исключением последнего параграфа, доступна учащимся десятого класса средней школы.

7. Хинчин А. Я., Цепные дроби, Издание второе, Гостехиздат, 1950.
Систематическое изложение теории цепных (непрерывных) дробей. Для чтения последней главы, посвящённой метрической теории цепных дробей, от читателя требуется знание интегрального исчисления и теории меры множеств.

8. Хинчин А. Я., Три жемчужины теории чисел, Издание второе, переработанное, Гостехиздат, М. — Л., 1948.
Брошюра посвящена доказательствам трёх глубоких теорем теории чисел (теорема об арифметической прогрессии, теорема о плотности суммы последовательностей чисел и теорема Варинга). Все эти доказательства были найдены за последнее десятилетие; они вполне элементарны, но всё же требуют от читателя большого внимания и уменья сосредоточиваться.

9. Кузьмин Р. О. и Фаддеев Д. К., Арифметика и алгебра комплексных чисел, Учпедгиз, Л., 1939.
Первая часть этой книги содержит алгебру комплексных чисел, а также определение и свойства элементарных функций комплексного переменного и понятие о кватернионах; вторая, меньшая, часть посвящена теории делимости целых рациональных чисел, целых комплексных чисел, чисел вида $a + b\rho$, где a и b — целые, а ρ — комплексный кубичный корень из единицы, и наконец, дальнейшим обобщениям теории делимости. Почти весь материал этой второй части в более сжатом изложении находится также в указанной выше брошюре Л. Г. Шнирельмана.

10. Хинчин А. Я., Великая теорема Ферма, ГТТИ, 1932.
Изложение в основном тексте брошюры не требует от читателя знакомства с теорией чисел. Лишь дополнение, содержащее относящиеся к теории алгебраических чисел исследования Куммера, предполагает хорошее владение основным курсом теории чисел.

В. М. БРАДИС

УСТНЫЙ И ПИСЬМЕННЫЙ СЧЁТ. ВСПОМОГАТЕЛЬНЫЕ СРЕДСТВА ВЫЧИСЛЕНИЙ

*

ГЛАВА I

ОБЩИЕ СВЕДЕНИЯ О СЧЁТЕ И ПРИБЛИЖЁННЫХ ВЫЧИСЛЕНИЯХ

§ 1. Общие соображения об изучении счёта в школе

Слово «счёт» употребляется в двух смыслах. Во-первых, счёт как операция, имеющая целью установить, сколько элементов содержит данное конечное множество; во-вторых, счёт как совокупность первых четырёх арифметических действий, производимых над рациональными числами целыми и дробными, т. е. счёт-вычисление. В настоящей статье речь идёт о счёте-вычислении, но, кроме первых четырёх арифметических действий, имеются в виду и некоторые другие операции над числами, с которыми имеет дело курс математики в средней школе.

Изучению счёта посвящён почти целиком курс математики I—V классов советской школы. Действующая ныне программа предполагает, что окончившие пять классов нуждаются по части счёта только в усвоении логарифмического метода вычислений, которому уделяется довольно много времени в IX классе, и никаких других вопросов, относящихся к теории и практике вычислений, не затрагивает. Не двигаясь в старших классах в этом направлении вперёд, учащиеся постепенно частично теряют и те немногие вычислительные знания и навыки, какие они приобрели в младших классах, и естественно, что вузы, особенно технические, нередко жалуются на недостаточную подготовку оканчивающей среднюю школу молодёжи в области вычислительной культуры.

Изучая математику, нельзя не рассматривать практических её приложений, а заключительной стадией решения любого практического вопроса, требующего применения математики, являются численные выкладки. Научить производить такие выкладки правильно, быстро, без напрасной траты времени и сил — несомненно, одна из задач общеобразовательного курса математики. Некоторый минимум хороших и прочных навыков вычислительной работы нужен каждому культурному человеку. Этот минимум существенно расширяется для всех технических специальностей, в том числе и для большинства

военных, для всех физико-математических, а в несколько меньшей мере и для всех естественно-научных дисциплин. Не следует также упускать из вида и воспитательное значение правильно поставленной вычислительной работы. На ней особенно хорошо развивается чувство ответственности, вырабатываются навыки самоконтроля, умения обнаруживать и исправлять свои ошибки, умения сосредоточенно работать, надлежащим образом рационализируя каждый свой шаг.

В области вычислительной техники наша средняя школа отстаёт от жизни. К примитивным арифметическим навыкам она добавляет только умение пользоваться логарифмическим методом вычисления. Между тем применение логарифмов давно уже потеряло тот универсальный характер, какой оно имело в XVIII и XIX вв.: на смену логарифмам пришли счётная логарифмическая линейка, получившая за последние полвека самое широкое распространение во всех случаях, когда точность в 3—4 значащих цифры оказывается достаточной, и различные счётные машины, дающие возможность получать результаты с произвольно высокой точностью, а также номограммы, поразительно ускоряющие работу вычисления по определённым формулам.

Существует ряд математических таблиц, вполне доступных даже учащимся семилетней школы и существенно облегчающих повседневную вычислительную работу, но фактически используемых в школе очень редко (таблица квадратов, кубов, корней квадратных и кубических, обратных значений, длины окружности, площади круга и др.).

Есть ещё одна важная сторона этого отрыва школьной вычислительной математики от жизни. Школа учит операциям над числами, которые предполагаются точными, между тем как в подавляющем большинстве случаев числа, с которыми приходится иметь дело на практике, лишь приближённо выражают точные, но неизвестные нам значения реальных величин. Можно точно сосчитать количество предметов в небольшом их собрании, но уже точный подсчёт более или менее значительного их множества представляет серьёзные, часто непреодолимые затруднения, и приходится довольствоваться выяснением лишь приближённых значений численности таких множеств. Что же касается измерений, то они всегда дают только приближённые значения измеряемых величин. В связи с этим неизбежно возникают такие вопросы: как оценить точность данного приближённого числа (т. е. числа, приближённо выражающего точное значение рассматриваемой величины)? Как оценить точность результата вычисления с приближёнными числами? Какова должна быть точность данных, чтобы результат вычисления с ними имел некоторую наперёд указанную точность? Как наиболее рационально производить действия над приближёнными числами?

На все эти вопросы школьный курс математики ответа не даёт. Представляется совершенно необходимым значительное обновление

школьных программ в разделах, посвящённых вычислительной работе, и нет сомнения, что это обновление не за горами. Но и в рамках действующих ныне программ учитель может сделать многое для повышения вычислительной культуры своих учеников, если, разумеется, сам обладает соответствующими знаниями и навыками.

Краткому обзору этого материала и посвящается настоящая статья. Три ближайших её параграфа рассматривают точные вычисления, все последующие — вычисления приближённые. Объём статьи заставляет ограничиваться лишь идейной, принципиальной стороной затрагиваемых вопросов и минимумом поясняющих примеров. Читателя, желающего ознакомиться с деталями, приходится отсылать к литературе, указанной в конце статьи. Ссылки на литературу делаются в тексте статьи посредством указания соответствующих номеров в прямоугольных скобках.

§ 2. Счёт устный

Общепринятые в настоящее время приёмы выполнения арифметических действий над многозначными натуральными числами, выраженными в десятичной системе счисления, сводятся в конечном итоге к применению табличек сложения и умножения однозначных чисел, заучиваемых наизусть, и предполагают запись данных, а также постепенную запись получаемых результатов как промежуточных (например, частных произведений при умножении), так и окончательных. Счёт называется «устным» или «умственным», если он ведётся без какой бы то ни было записи. Навыки такого счёта представляют собой большую ценность и в чисто практическом отношении, так как используются в быту несравненно чаще, чем письменные выкладки, и в отношении развития тех способностей, какие культивируются изучением математики вообще: сообразительности, внимательности, инициативы и т. д. В то время как обычные письменные вычисления производятся по строго определённым правилам и представляют собой работу в значительной степени механическую, устный счёт оставляет большой простор для изобретательности и наблюдательности и предъявляет серьёзные требования к вниманию и навыкам самоконтроля. Промежуточное положение между устным и письменным счётом занимает счёт «полуписьменный», когда записываются только данные и окончательный результат. Резкой границы между устным и полуписьменным счётом провести, однако, нельзя, и мы не будем в дальнейшем различать их.

Обычно в I—IV классах учащиеся овладевают простейшими приёмами устного счёта над натуральными числами, не превосходящими 100, и над дробями с такими знаменателями, как 2, 4, 8, 3, 6, 10. В дальнейшем эти навыки не развиваются и даже не используются, а в силу этого естественно теряются. Нередко мы видим, как выпускники средней школы тянутся за карандашом и бумагой,

чтобы найти сумму двух двузначных натуральных чисел. Представляется целесообразным выдвинуть относительно устного счёта следующие три требования.

а) Необходимо приучать учащихся всех классов средней школы выполнять в уме всякую выкладку, где это возможно без особого напряжения, в частности, производить в уме все четыре действия над натуральными числами в пределах ста. Наибольшие трудности доставляет здесь умножение двузначных чисел, но и они преодолеваются при небольшой тренировке в применении известного правила «умножения крест-на-крест». Например, умножая 53 на 74, сначала берут произведение единиц ($3 \cdot 4 = 12$), цифру 2 записывают, а один десяток запоминают; далее находят произведение десятков на единицы ($5 \cdot 4 = 20$) и единиц на десятки ($3 \cdot 7 = 21$), берут сумму $1 + 20 + 21 = 42$ (десятка), цифру 2 записывают левее уже записанной цифры 2, цифру 4 (сотни) запоминают; наконец, находят произведение десятков на десятки ($5 \cdot 7 = 35$) и сумму $35 + 4 = 39$ записывают левее записанного ранее числа 22, получая в итоге произведение 3922.

Конечно, здесь, как и везде, должна соблюдаться разумная мера.

б) Желательно всячески культивировать разнообразные частные приёмы устного счёта, использующие индивидуальные свойства чисел, а также законы переместительный, сочетательный, распределительный и изменение результатов в зависимости от изменения данных. Подобные приёмы дают весьма заметную экономию (не только мела, а и мозговой энергии!) по сравнению с общими приёмами. Вот несколько примеров (подробная запись приведена только с целью разъяснения приёмов):

$$32\,704 \cdot 25 = 3\,270\,400 : 4 = 817\,600,$$

так как

$$a \cdot 25 = (a \cdot 100) : 4;$$

$$47 + 48 + 49 + 50 + 51 + 52 + 53 + 54 =$$
$$= (47 + 54) + (48 + 53) + (49 + 52) + (50 + 51) = 101 \cdot 4 = 404;$$

$$735 + 99 = 735 + 100 - 1 = 835 - 1 = 834;$$

$$15\tfrac{1}{2} + 32\tfrac{7}{16} + 1\tfrac{1}{3} + 2\tfrac{1}{6} =$$
$$= (15 + 32 + 1 + 2) + \left(\tfrac{1}{2} + \tfrac{1}{3} + \tfrac{1}{6}\right) + \tfrac{7}{16} = 50 + 1 + \tfrac{7}{16} = 51\tfrac{7}{16};$$

$$14\tfrac{3}{4} \cdot 8 = \left(14 + \tfrac{3}{4}\right) \cdot 8 = 14 \cdot 8 + \tfrac{3}{4} \cdot 8 = 112 + 6 = 118;$$

$$135\tfrac{3}{7} : 15 = \left(135 + \tfrac{3}{7}\right) : 15 = 135 : 15 + \left(\tfrac{3}{7} : 3\right) : 5 = 9 + \tfrac{1}{7} : 5 = 9\tfrac{1}{35}.$$

в) Желательно пополнять этот запас частных приёмов, используя по мере ознакомления с ними различные формулы алгебры, а также выводя некоторые новые практически ценные формулы. Вот несколько примеров:

$$54 \cdot 46 = (50 + 4) \cdot (50 - 4) = 50^2 - 4^2 = 2484;$$

$$97^2 = (100 - 3)^2 = 10\,000 - 600 + 9 = 9409;$$

при $b + c = 10$

$$(10a + b)(10a + c) = 100a(a + 1) + bc,$$

а потому, например,

$$9993 \cdot 9997 = 100 \cdot 999 \cdot 1000 + 3 \cdot 7 = 99\,900\,021;$$

$$82 \cdot 88 = 100 \cdot 8 \cdot 9 + 16 = 7216;$$

$$(10 + a)(10 + b) = 100 + 10(a + b) + ab,$$

поэтому, например,

$$13 \cdot 16 = 100 + 10 \cdot 9 + 18 = 208;$$

иначе

$$13 \cdot 16 = 16 \cdot 10 + 16 \cdot 3 = 160 + 48 = 208;$$

$$\sqrt{74^2 - 70^2} = \sqrt{144 \cdot 4} = 12 \cdot 2 = 24.$$

Отметим в заключение настоящего параграфа следующее правило, которого с большой выгодой для воспитания хороших вычислительных навыков придерживаются некоторые учителя: учащиеся любого класса, выполняя каждую числовую выкладку, начинают с грубо приближённой оценки искомого результата, округляя все данные до одной-двух значащих цифр и выполняя все действия в уме. Так, если требуется найти

$$x = \sqrt{0{,}0045 \cdot 7{,}5132 : (2{,}0719 \cdot 0{,}864)},$$

то сначала в уме находят:

$$x \approx \sqrt{0{,}004 \cdot 8 : (2 \cdot 0{,}9)} = \sqrt{0{,}016 : 0{,}9} = \sqrt{0{,}16 : 9} = 0{,}4 : 3 \approx 0{,}13,$$

а затем уже письменно получают более точное значение (в данном случае, если ограничиться четырьмя значащими цифрами, $x \approx 0{,}1374$). Такая «прикидка» существенно предупреждает грубые просчёты и очень ценится инженерно-техническими работниками.

Желающим детальнее изучить приёмы устного счёта рекомендуется обратиться к работам [1], [2а], [3], [4].

§ 3. Счёт письменный

С письменными выкладками над числами как целыми, так и дробными дело в школе обстоит несравненно благополучнее, чем с устным счётом. Изучаемые в школе общепринятые в настоящее время алгорифмы (схемы выполнения и записи) действий над многозначными числами являются лучшими из многочисленных предложенных в разное время вариантов; усваиваются они в подавляющем большинстве случаев достаточно твёрдо ещё в начальной школе. Обычный курс математики семилетней и средней школ даёт достаточно случаев применять их и обеспечивает сохранение технических навыков. По поводу письменного производства действий над многозначными целыми числами можно высказать всё же несколько пожеланий методического характера.

а) Знакомя учащихся с переместительным, сочетательным, распределительным свойствами суммы и разности, надо выяснять, как эти свойства используются в обычных алгорифмах сложения и вычитания многозначных чисел; делается это либо при повторении арифметики, либо на первых шагах изучения алгебры. Весьма важно, чтобы учащиеся не только безупречно владели механизмом действия, но и понимали бы теоретическую базу этого алгорифма, остающуюся по необходимости далеко не полностью уяснённой при первоначальном знакомстве с этим действием. Весьма поучительно проведение подобной работы и над действиями умножения и деления.

б) Требуя аккуратной записи всегда и везде, приходится обращать особое внимание на эту сторону дела при выполнении действий над многозначными числами и над дробями. Нельзя допускать небрежной записи выкладок в черновиках; такая запись — один из постоянных источников ошибок, механически повторяемых при переписке набело.

в) Требуя от учащихся, чтобы они не допускали вычислительных ошибок, надо приучать их к рациональным способам проверки своих выкладок. Никакое вычисление нельзя считать законченным, пока не сделана тем или иным способом проверка. Сложение обычно проверяют сложением же, но выполняемым в ином порядке; вычитание — сложением, умножение — умножением же (при перемене мест сомножителей), деление — умножением делителя на частное и прибавлением остатка, если он есть, извлечение корня — возведением в степень.

Очень полезна проверка с помощью чисел 9 и 11, основанная на замене данных их остатками от деления соответственно на 9 и 11: выполняя над этими остатками указанные действия, мы получаем в случае безошибочности всех выкладок числа, дающие при делении на 9 и 11 те же остатки, что и найденные результаты. Числа 9 и 11 берутся делителями в силу того, что при делении на них остатки находятся особенно просто: остаток от деления

на 9 любого числа, записанного в десятичной нумерации, одинаков с остатком от деления на 9 суммы цифр этого числа. Так, остаток от деления на 9 числа 4 138 097 одинаков с остатком от деления на 9 числа $4+1+3+8+0+9+7=32$ и с остатком от деления на 9 числа $3+2=5$. Остаток от деления на 11 любого числа, записанного в десятичной нумерации[1]), получается подобным же образом через вычисление «альтернирующей» суммы цифр этого числа, т. е. суммы его цифр, взятых с чередующимися знаками, начиная с цифры единиц (чтобы избежать появления отрицательных чисел, можно прибавлять 11 каждый раз, когда от меньшего числа приходится отнимать большее). Например, остаток от деления числа 4 138 097 на 11 равен остатку от деления на 11 числа $7-9+0-8+3-1+4+11=7$. Подробности о проверке девяткой можно найти в книге [5].

Отсутствие грубых просчётов легко устанавливается посредством той легко выполнимой в уме «прикидки», о которой было упомянуто выше и которую рекомендуется производить раньше полного вычисления.

г) Отметим несколько распространённых ошибок, совершаемых при письменном выполнении действий над целыми и дробными числами. Часто пропускаются нули в промежуточных разрядах частного. Например, при делении 3708 на 18 получают частное 26 вместо 206. Любопытно, что подобные ошибки не встречаются при устном выполнении действия, в данном случае так легко осуществляемом: $3708:18=(3600+108):18=200+6=206$.

Нередко искажают остаток при зачёркивании конечных нулей в делимом и делителе. Например, при делении 650 на 110 заменяют эти числа через 65 и 11 и получают правильное частное 5 и неверный остаток 10 (вместо 100).

Очень часто без всякой надобности практикуется обращение в неправильные дроби данных смешанных чисел при сложении и вычитании таких чисел. Результат от такого обращения не искажается, но выкладки существенно усложняются.

Иногда при умножении смешанных чисел ограничиваются умножением целого на целое и дроби на дробь. Например, при умножении $5\frac{2}{3}$ на $2\frac{3}{4}$ получают $5\cdot 2=10$ и $\frac{2}{3}\cdot\frac{3}{4}=\frac{1}{2}$, всего $10\frac{1}{2}$, тогда как правильный результат есть $\frac{17\cdot 11}{3\cdot 4}=15\frac{7}{12}$.

Нечего и говорить, как поучителен основательный разбор этих и других подобных им ученических вычислительных ошибок.

д) При всяком сколько-нибудь сложном письменном вычислении делом большой важности является рациональная запись выкладок.

Неряшливая, разбросанная запись абсолютно недопустима ни при каких обстоятельствах, в том числе и в черновике. Запись должна

[1]) См. стр. 274—275, А. Я. Хинчин, «Элементы теории чисел».

быть ясной: не только сам вычисляющий, но и другой человек должен иметь возможность легко в ней разобраться. Она должна быть достаточно полной, но экономной, содержа всё необходимое и ничего излишнего. Очень полезно предварительное составление с х е м ы, т. е. такая разметка листа бумаги, производимая до вычисления, при которой каждое получаемое в процессе вычисления число попадает на своё, вполне для него определённое место. Те вспомогательные вычисления, какие нельзя выполнять в уме, проводятся на особом отведённом для них месте. Желательны указания на в с п о м о г а т е л ь н ы е с р е д с т в а вычислений (таблицы, приборы, графики), какие в данном вычислении были использованы. Необходимой заключительной частью всякого вычисления является п р о в е р к а, а также соображения о т о ч н о с т и полученного результата, так как в подавляющем большинстве случаев результат вычисления даже при точных данных бывает только приближённым (этим вопросом будем ещё заниматься в дальнейшем). Если выполненное вычисление переписывается набело, рекомендуется проверять каждую его цифру, находя её с целью проверки заново и сравнивая с черновиком.

Вот пример записи решения задачи (для IX класса).

З а д а ч а. Найти длину x стороны квадрата, равновеликого треугольнику со сторонами $a = 89$ *м*, $b = 321$ *м*, $c = 395$ *м*.

Р е ш е н и е г р а ф и ч е с к о е (в масштабе: в 1 клетке 20 *м*). Построив по трём данным сторонам $\triangle ABC$ (рис. 1), проводим $CD \perp AB$ и откладываем на продолжении AB отрезок $BE = 0{,}5\ CD$,

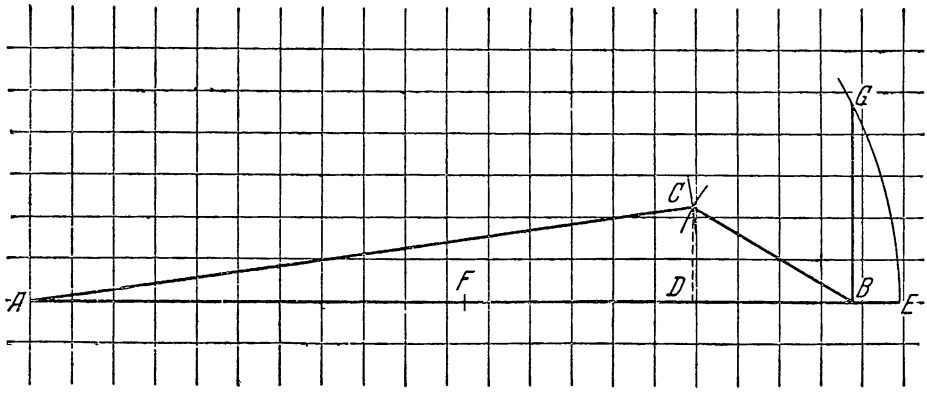


Рис. 1.

затем строим окружность на отрезке AE, как на диаметре. Полухорда BG, проведённая перпендикулярно к AE, представляет собой искомый отрезок. Его длина 4,8 клетки, а потому ответ $x \approx 96$ *м*. Цифра единиц здесь ненадёжна, так как вполне возможна ошибка при измерении BG в 0,1 клетки, т. е. в 2 *м*.

Р е ш е н и е в ы ч и с л и т е л ь н о е. Формулы:

$$s^2 = p(p-a)(p-b)(p-c);\ 2p = a+b+c;\ x = \sqrt{s}.$$

Вычисление по таблице четырёхзначных логарифмов.

a	89
b	321
c	395
$2p$	805
p	402,5
$p-a$	313,5
$p-b$	81,5
$p-c$	7,5
$(p-a)+(p-b)+(p-c)=$	402,5
$=3p-2p=p$	(контроль)

$\lg p$	2,6047
$\lg(p-a)$	2,4962
$\lg(p-b)$	1,9112
$\lg(p-c)$	0,8751
$\lg s^2=\lg x^4$	7,8872
$\lg x$	1,9718
x	93,72

Ответ $x\approx 93{,}72$.

Если данные — числа точные, то в ответе можно ручаться за первые три значащие цифры, четвёртая же ввиду использования четырёхзначных логарифмов не вполне надёжна.

Как видим, получилось удовлетворительное согласие между обоими решениями. Контрольное вычисление, проведённое посредством семизначных логарифмов, даёт $x\approx 93{,}71424$.

Вопросу о рационализации записи вычислений и вообще записи решений задач уделяется в школе мало внимания. Надо давать хорошо продуманные образцы записи, но отнюдь не требовать слепого подражания им, а мобилизовать учащихся на дальнейшее их улучшение.

§ 4. Вспомогательные средства вычисления

В настоящее время весьма широкое распространение получили разнообразные приборы и машины, автоматически или полуавтоматически выполняющие многие математические операции, начиная от сложения (и вычитания) многозначных чисел, с таким успехом выполняемого на всем известных русских (конторских) счётах, до решения самых сложных вычислительных задач гармонического анализа и интегрирования уравнений в частных производных, производимого сконструированными и построенными в СССР машинами, каждая из которых заменяет десятки квалифицированных вычислителей. Допустимо ли, чтобы школьная математика полностью игнорировала это полезнейшее дело механизации счётной работы? Даже в рамках семилетней школы вполне возможно использование трёх рассмотренных ниже простейших средств механизации вычислений (счёты, палочки Непера, арифмометр). Счётная логарифмическая линейка, сделавшаяся теперь необходимой принадлежностью каждого инженера и техника, должна войти в обиход учащихся IX и X классов. Желательно, чтобы сам учитель постоянно ею пользовался как в своей

домашней работе, так и на глазах учащихся любого класса. Об этом приборе речь будет идти в § 17.

Счёты представляют собой прекрасное средство для производства действий сложения и вычитания многозначных чисел, с успехом конкурирующее, пока речь идёт об этих двух действиях, в отношении скорости работы с арифмометром наиболее распространённого типа. Дело в том, что на арифмометре надо при сложении и вычитании устанавливать последовательно каждое данное, а затем прибавлять или вычитать его вращением рукоятки, на счётах же особой установки требует только первое данное. Конечно, счёты не дают полной автоматизации: перенос десятков, т. е. замена каждых десяти косточек, накопившихся на одной спице, одной косточкой следующей спицы, как и аналогичная операция при вычитании, требует внимания вычислителя и является главным источником ошибок. Тем не менее счёты так экономят время, нужное для выполнения сложения и вычитания, и так просты по своему устройству и употреблению, что получили в нашей практике самое широкое применение. Уже окончившие начальную школу должны согласно действующей ныне программе владеть навыками работы на счётах. Средняя школа, к сожалению, счёты не использует. Желательно, чтобы навыки использовались и закреплялись в средней школе, тем более, что постоянное пользование счётами доставит заметную экономию времени, затрачиваемого на решение задач, особенно в V классе. Умножение, как последовательное сложение, и деление, как последовательное вычитание, тоже с успехом выполняются на счётах (с различными упрощениями в частных случаях; так, например, умножить 365 на 17 на счётах можно согласно записи $3\,650 + 3\,650 - 365 - 365 - 365$). Это, однако, представляет большие трудности; на первых порах следует ограничиться только сложением и вычитанием.

В той же неполной, но всё же значительной мере, в какой сложение и вычитание механизируются благодаря счётам, действия умножения и деления механизируются благодаря применению весьма простого, но мало распространённого прибора — палочек Непера. Это — набор полосок, изображённый на рис. 2, причём каждая полоска должна быть в нескольких экземплярах. Полоски имеют сверху цифры от 0 до 9, а ниже — произведения этого числа на все однозначные числа, причём в каждом произведении цифра десятков записывается несколько выше и левее цифры единиц, отделяясь от неё наклонной чертой. Желая умножить, например, число 37 214 на какое угодно другое натуральное число, укладываем рядом палочки с цифрами 3, 7, 2, 1, 4 в заголовках, как показано на рис. 3, и читаем на последовательных строках произведения данных чисел на 1, 2, 3, ..., 9, причём необходимый перенос десятков делается в уме. Сначала эти произведения читаются справа налево. Например, произведение 37 214 на 7 содержит 8 единиц, $7 + 2 = 9$ десятков, $4 + 0 = 4$ сотни, $9 + 1 = 10$ тысяч, $1 + 1 + 4 = 6$ десятков тысяч, 2 сотни

тысяч. Однако быстро приобретается навык в чтении произведений сразу слева направо. Таким образом, палочки Непера дают готовые произведения любого числа на все однозначные. Чтобы умножить многозначное на многозначное, надо выложить на палочках множимое, взять с них готовые частные произведения, надлежащим образом подписать их друг под другом и сложить их. Присоединяя к палочкам Непера счёты, мы ещё больше механизируем умножение: записывать приходится только окончательный результат.

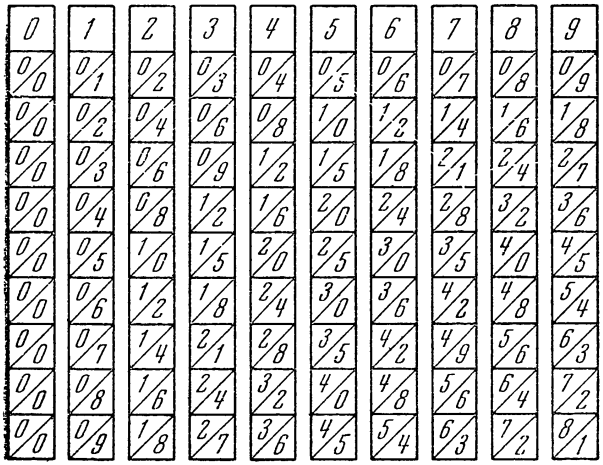


Рис. 2.

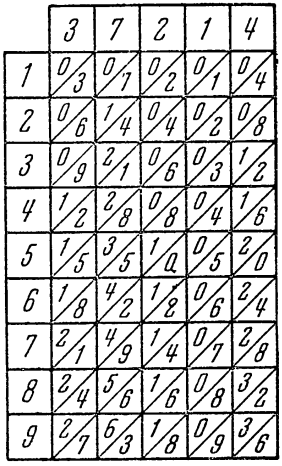


Рис. 3.

Несравненно дальше, чем при применении счётов и палочек Непера, идёт механизация арифметических действий при использовании арифмометра «Феликс», названного так в честь Ф. Э. Дзержинского и изготовляемого на советских заводах. Эта счётная машина изображена на рис. 4. Она представляет собой дальнейшее усовершенствование машины, которую в конце XIX в. построил петербургский инженер В. Т. Однер. Арифмометр получил у нас самое широкое распространение, имеется почти в каждом учреждении. Усвоение принципа устройства арифмометра и техники работы требует всего 15—20 минут, и крайне желательно, чтобы каждый оканчивающий среднюю школу умел на нём работать. В то время как применение палочек Непера ускоряет производство умножения и деления примерно вдвое, арифмометр даёт ускорение примерно в 10—12 раз (по сравнению с обычным письменным производством этих действий на бумаге). Вычисление, требующее без применения арифмометра целого часа работы, с его помощью выполняется в 5—6 минут, притом с несравненно меньшими шансами сделать ошибку.

Приводим заимствованное из книги автора [2а] описание устройства арифмометра «Феликс» и работы на нём.

Верхнюю часть машины образует установочный механизм. На рис. 4 видны концы 9 спиц, принадлежащих установочному механизму и способных перемещаться вдоль 9 прорезов. На левом краю каждого прореза имеются цифры от 0 до 9, идущие сверху вниз. Двигая рукой спицы, можно установить посредством них любое девятизначное число, целое или дробное десятичное, причём знаком дробности служит металлическая «запятая», которую можно устанавливать между верхними концами любых двух соседних прорезов. Направо от установочного механизма имеется рукоятка с ручкой. Чтобы повернуть рукоятку, надо сначала оттянуть ручку немного вправо, сделать, далее, тре-

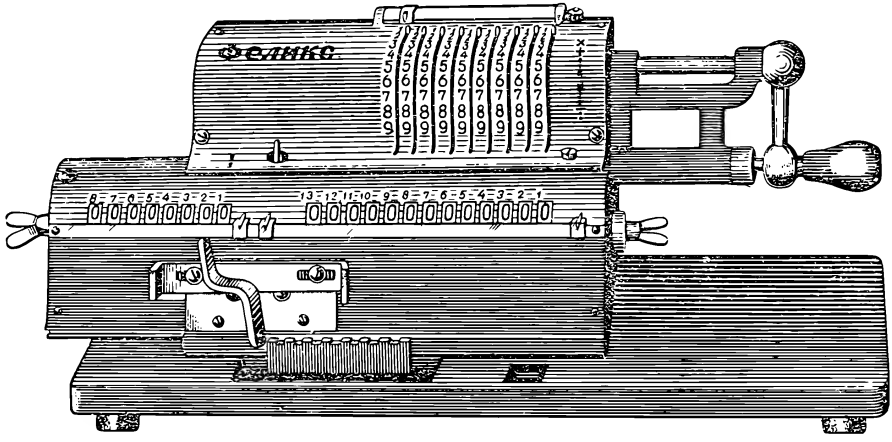


Рис. 4.

буемое число полных оборотов, а затем обязательно привести рукоятку в то «нормальное» положение, какое показано на рисунке. Ниже установочного механизма находится каретка, снабжённая двумя рядами окошек: справа видны 13 окошек, которые будем называть *ответными окошками*, так как в них появляются результаты действий сложения, вычитания и умножения, а слева — 8 окошек счётчика оборотов, которые будем называть *счётными окошками*. На левом и правом концах каретки видны две ласточки, вращение которых заменяет нулями («гасит») те цифры, какие появляются в счётных и ответных окошках. По планке под окошками скользят металлические запятые, а ниже планки находится приспособление (транспортёр), позволяющее передвигать каретку либо на величину одного только интервала между соседними прорезами установочного механизма, либо на несколько таких интервалов сразу.

Прежде чем вращать рукоятку, надо всегда убедиться, что обе ласточки каретки приведены в горизонтальное положение (достигая этого положения, ласточка щёлкает) и что средняя планка транспортёра находится против одного из промежутков между зубцами расположенной ниже гребёнки (транспортёр тоже должен щёлкнуть).

Если хотя бы одно из этих условий не соблюдено, рукоятка вращаться не будет, а попытка всё же повернуть её приведёт немедленно к поломке машины. На уровне нижних концов прорезов установочного механизма и несколько левее их видна кнопка, назначение которой — ускорять приведение спиц в нулевое положение: подвинув эту кнопку влево и одновременно осторожно вращая рукоятку к себе, мы после возвращения рукоятки к нормальному положению будем иметь все спицы на нулях. Надо только помнить, что после одной трети оборота рукоятки, когда все спицы будут «выравнены», кнопку надо отпускать. Правее крайнего правого прореза на кожухе машины видны две стрелки, направленные в противоположные стороны и снабжённые знаками действий (одна $+$ и $\times$, другая — и :). Эти стрелки указывают направления, в каких надо вращать рукоятку при выполнении различных действий. Будем называть эти направления *положительным* (из нормального положения ручки к себе) и *отрицательным* (от себя).

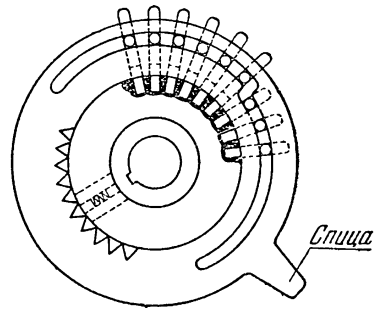


Рис. 5.

Мы рассмотрели все части машины, с которыми приходится иметь дело при вычислении. Внутреннего её устройства касаться не будем, укажем только, что основным её элементом является «зубчатка Однера», изображённая на рис. 5. Эта зубчатка имеет переменное число выступающих наружу зубцов, а именно столько, на сколько делений своего прореза опущена соответствующая спица. На рис. 5 зубчатка имеет шесть выступающих зубцов, остальные спрятаны. Двигая спицу, мы меняем число зубцов в той зубчатке, которая с этой спицей связана, от 0 до 9. Зубчаток Однера в арифмометре столько, сколько спиц.

Поставив в первом (крайнем правом) прорезе спицу на цифру 3 и сделав поворот рукоятки в положительном направлении, мы повернём на три зубца колесо, на ободе которого нанесены цифры, видные через первое (крайнее правое) ответное окошко. Если раньше в этом окошке была видна цифра 0, то теперь появится 3. Второй поворот рукоятки в том же направлении повернёт это колесо ещё на три зубца, и вместо цифры 3 мы увидим в ответном окошке уже цифру 6: мы выполнили сложение $3+3$ или, что то же, умножение $3 \cdot 2$. Новый поворот рукоятки даёт уже $6+3=9$ или $3 \cdot 3=9$. При четвёртом повороте рукоятки в первом ответном окошке пройдут последовательно цифры 9, 0, 1, 2 (колесо сделало полный оборот и начинает делать второй), а затем во втором ответном окошке (рядом) появится цифра 1. Здесь приходит в действие механизм переноса десятков, являющийся самой деликатной частью всякой счётной машины. В итоге получаем $9+3=12$ или $3 \cdot 4=12$.

Теперь нетрудно понять, как выполняются на рассматриваемой машине четыре основных действия. Чтобы сложить два числа, надо: 1) поставить нули в ответных окошках (вращая до щелчка правую ласточку), 2) установить на спицах первое слагаемое (последнюю его цифру обычно ставят посредством первой, т. е. крайней правой спицы, но это не обязательно), 3) перевести это слагаемое в ответные окошки (одним поворотом рукоятки к себе), 4) установить на спицах второе слагаемое, 5) сделать ещё один поворот рукоятки к себе; теперь в ответных окошках появится искомая сумма. Те же пять операций производятся и для выполнения вычитания, но после установки на спицах вычитаемого рукоятка вращается в обратном направлении. Понятно, что к полученному числу можно прибавить (или от него отнять) ещё сколько угодно чисел.

Умножение на однозначное число выполняется как повторное сложение: чтобы умножить, например, на 9, вращаем рукоятку 9 раз к себе. Для умножения на двузначное число, например 39, используется возможность перемещения каретки относительно верхней части машины, содержащей установочный механизм: переместив каретку посредством транспортёра на один интервал вправо, вращаем рукоятку три раза к себе и получаем в ответных окошках произведение взятого числа на 30. Теперь остаётся вернуть каретку в нормальное положение, когда первое ответное окошко находится под первым прорезом, и сделать ещё 9 оборотов рукоятки к себе. В ответных окошках получим искомое произведение на 39.

Умножение на 39 описанным способом требует $3+9=12$ оборотов рукоятки; это число уменьшится до 5, если при сдвинутой направо каретке сделать не 3, а 4 оборота, т. е. умножить на 40, а затем, вернув каретку в нормальное положение, сделать один оборот в обратную сторону (от себя). Этот приём употребляется на практике и позволяет никогда не вращать рукоятку более 5 раз подряд в одну сторону, так как умножение на 9, 8, 7, 6 заменяется умножением на 10 и вычитанием 1-, 2-, 3-, 4-кратного множимого.

Число сделанных оборотов рукоятки регистрируется в счётных окошках (слева). Выполняя умножение, надо предварительно привести к нулю все цифры счётных окошек вращением до щелчка левой ласточки. Таким образом, правило умножения можно формулировать так: установив множимое на спицах, комбинируй движение каретки и вращение рукоятки так, чтобы в счётных окошках получить множитель; тогда в ответных окошках получится произведение. Нужно только иметь в виду, что при вращении рукоятки в отрицательном направлении в счётных окошках появляются красные цифры и набирать в них делитель надо в особой форме. Так, при умножении на 39, как 40—1, в ответных окошках должно быть число $4\bar{1}$, где знаком $\bar{1}$ мы условно изображаем красную цифру 1. При умножении на число 8376 в счётных окошках должно быть число $1\bar{2}\,4\bar{2}\bar{4}$, где $\bar{2}$

и $\overline{4}$ опять условно обозначают красные цифры. Пользуясь красными цифрами, мы в этом случае должны будем повернуть рукоятку $1+2+4+2+4=13$ раз, тогда как без них понадобилось бы $8+3+7+6=24$ оборота.

Выполняя на арифмометре умножение как повторное сложение, можно выполнить на нём деление как повторное вычитание. Разделить, например, 17 на 3 — значит узнать, сколько раз можно отнимать от 17 число 3 (до получения остатка, меньшего делителя). Поэтому делимое устанавливают в ответных окошках, делитель — на спицах, и начинают вычитать. Частное как число сделанных оборотов получается в счётных окошках. При делении многозначных чисел, как и при умножении, для уменьшения числа оборотов рукоятки используется движение каретки. Пусть, например, требуется разделить 243 558 на 913. Устанавливаем делимое в крайних левых ответных окошках; в остальных ответных окошках, как и во всех счётных окошках, должны быть нули. Отделяя посредством металлической запятой первые три цифры делимого (по числу цифр делителя), мы замечаем, что получилось число 243, меньшее делителя; поэтому берём ещё одну цифру, т. е. отделяем число 2435. Сдвинув каретку до отказа вправо, устанавливаем делитель 913 на спицах так, чтобы его можно было отнимать от 2435 (цифра 9 должна быть над цифрой 4), и делаем вычитание столько раз, сколько возможно, т. е. пока не получим в остатке числа, меньшего делителя. Получив после двух оборотов рукоятки в остатке число 609, смещаем каретку на одно место влево, а запятую — на одно место вправо и повторяем операцию. После 6 оборотов рукоятки получаем остаток 617. Смещая каретку ещё на одно место влево, а запятую вправо, вновь делаем последовательное вычитание, пока не получим после шести оборотов остатка 700. Деление в целых числах окончено: частное 266 получено в счётных окошках, остаток 700 — в ответных окошках. Продолжая те же операции, мы получим десятые, сотые и т. д. доли частного.

Выполняя деление, можно не следить за последовательно получаемыми остатками, а крутить рукоятку до звонка, который машина даёт при первом лишнем обороте, и затем сделать один оборот к себе, уничтожая сделанный лишний оборот от себя.

Рассмотрим ещё извлечение квадратного корня.

Наиболее употребительный способ извлечения квадратного корня посредством арифмометра основан на легко проверяемом тождестве

$$1+3+5+7+\ldots+(2n-3)+(2n-1)=n^2,$$

говорящем, что сумма n первых последовательных нечётных натуральных чисел равна квадрату этого числа. Поэтому, чтобы извлечь из какого-нибудь натурального числа квадратный корень, надо вычитать из него последовательно числа 1, 3, 5, 7, ... до тех пор пока не получим в остатке число, меньшее очередного вычитаемого. Число

сделанных вычитаний и будет искомым квадратным корнем (точнее квадратным корнем из наибольшего точного квадрата, заключающегося в данном числе). Надлежащее перемещение каретки арифмометра и здесь позволяет во много раз уменьшить необходимое число вычитаний. Рассмотрим детали этого способа на примере.

Пусть требуется найти $\sqrt{5\,234\,096}$. Установив подкоренное число, как делимое при делении, в крайних левых ответных окошках (в остальных — нули) и погасив имеющиеся цифры в счётных окошках, смещаем каретку до отказа вправо и отделяем запятой старшую грань подкоренного числа (цифру 5). Начинаем вычитать из 5 нечётные числа и останавливаемся после двух вычитаний: $5 - 1 - 3 = 1$, — дальше вычитать нельзя. Смещаем затем каретку на одно место влево, а запятую в подкоренном числе — на два места вправо. Последнее вычитаемое (3) увеличиваем на 1 и ближайшую справа спицу ставим на 1. Продолжаем вычитать нечётные числа, начиная с 41. После двух оборотов останавливаемся, так как получается число $123 - 41 - 43 = 39$, из которого следующее нечётное число 45 вычитать уже нельзя. Опять смещаем каретку на одно место влево, а запятую на два места вправо; увеличиваем на 1 последнее вычитаемое 43 и рядом с ним ставим 1. Вычитаем, далее, нечётные числа, начиная с 441 и кончая 455 (восемь вычитаний). Смещаем каретку ещё на одно место влево, а запятую на два места вправо (теперь запятая оказывается после последней цифры остатка 36 696) и вычитаем последовательно числа 4561, 4563,..., 4573. Теперь в ответных окошках мы имеем окончательный остаток 3727, а в счётных окошках — искомый корень 2287. Для проверки находим

$$2287^2 + 3727 = 5\,234\,096$$

и убеждаемся, что всё правильно, так как

$$2288^2 = (2287 + 1)^2 = 2287^2 + 2 \cdot 2287 + 1 = 2287^2 + 4575$$

больше данного подкоренного числа.

Из других счётных машин, предназначенных, как и арифмометр «Феликс», для выполнения основных арифметических действий, отметим арифмометр с непрерывным движением, изобретённый и построенный знаменитым русским математиком П. Л. Чебышевым в 1882 г. При вращении каждого счётного колеса этой машины счётное колесо следующего высшего разряда вращается со скоростью, в 10 раз меньшей; передача десятков с одного разряда на другой совершается непрерывно; механизм для выполнения этой передачи проще, чем в машине, изобретённой Однером. Описание арифмометра Чебышева имеется в IV томе Полного собрания его сочинений[1]).

[1]) П. Л. Чебышев, Полное собрание сочинений, т. IV, Теория механизмов, Издательство АН СССР, 1948.

Существует ряд других машин, выполняющих четыре арифметических действия и носящих в отличие от других счётных машин общее название «вычислительных машин». Они различаются большей или меньшей степенью автоматизации работы с разными дополнительными устройствами: печатающими ответы, контролирующими правильность установки, дающими общий итог («наростающий итог») производимых суммирований и др. В СССР уже давно работает ряд заводов, выпускающих такие вычислительные машины, в то время как в дореволюционной России они вовсе не производились. Особое распространение получила клавишная счётная машина (сокращённо КСМ), изображённая на рис. 6. Вращение счётных колёс производится в ней не вручную, как в арифмометре «Феликс», а электрическим мотором, видным на рисунке слева; маленькая рукоятка предназначена только для гашения счётчиков. Машина начинает работать на сложение и умножение после нажатия клавиши со знаком плюс, на вычитание и деление — со знаком минус. Благодаря работе мотора КСМ даёт результаты значительно скорее, чем арифмометры, работающие вращением рукоятки от руки, и меньше утомляет вычислителя.

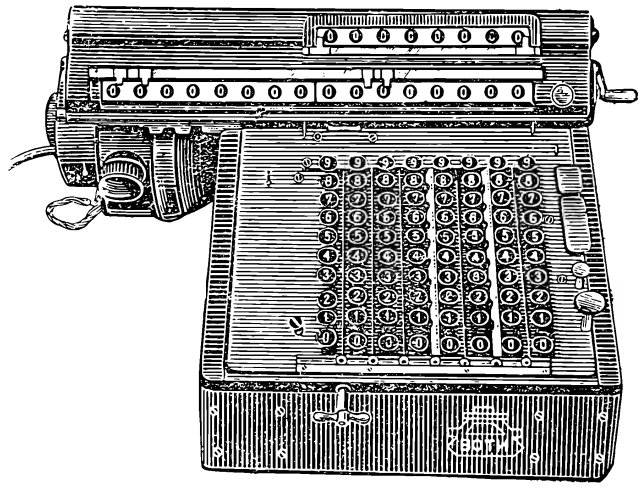


Рис. 6.

Вычислительные задачи, выдвигаемые различными науками и разными отраслями техники, особенно астрономией, оптикой, статистикой, оборонной техникой, привели к созданию многих типов счётных машин, несравненно более сложных и более совершенных, чем описанные выше вычислительные машины. Спроектировать и построить особую машину выгодно всякий раз, когда на практике такая задача многократно повторяется при различных исходных данных, особенно тогда, когда большое значение имеет, как это бывает, например, в задачах артиллерии, быстрота решения. Нередко такая машина представляет собой комбинацию нескольких более простых машин, каждая из которых выполняет одну определённую операцию и передаёт полученные результаты следующей машине, причём всё совершается автоматически. Таким образом насущные задачи науки и техники привели к созданию новой отрасли точного машино-

строения — к конструированию и производству различных «счётно-решающих устройств».

«В основе всякого счётно-решающего устройства, — пишут Н. Е. Кобринский и Л. А. Люстерник [1]), — лежит моделирование некоторой математической зависимости, создание такого физического процесса, который изображает эту зависимость. Операция сложения чисел, например, моделируется сложением угловых или линейных перемещений, сложением токов, сходящихся в узле электрической цепи, и т. д. Операции умножения можно моделировать изображением множителей в виде углового перемещения и длины плеча рычага, а произведения — линейным перемещением его конца; или множители изображают напряжение и проводимость, а их произведение на основе закона Ома — силу тока и т. д. ... Одна и та же математическая зависимость описывает разные физические процессы, и каждый из них может моделировать её. Естественно остановиться на том, который легче задать и состояние которого легче измерить... Интересно отметить, что в своё время строились механические модели для расчёта электрических цепей. Сейчас, с развитием измерительной электрической техники, построены электрические приборы, моделирующие механические системы».

Во многих случаях важно найти площадь плоской фигуры, ограниченной произвольным контуром. Геодезист делает это на плане, инженер-энергетик — на индикаторной диаграмме, показывающей зависимость давления в цилиндре паровой машины или двигателя внутреннего сгорания от положения поршня; на кожевенных заводах учитывают продукцию обмером площади каждой выделанной кожи. Для упрощения и ускорения решения этой задачи построено много специальных приборов, известных под названием «планиметров» и представляющих собой счётно-решающие устройства непрерывного действия. Работают они автоматически, позволяя отсчитать искомый результат непосредственно после того, как обводный штифт прибора обойдёт весь данный контур по чертежу, или после того, как обмеряемый контур (например, контур выделанной кожи) будет пропущен между валками прибора.

Всевозможные задачи на дискретные (не непрерывные) величины, сводящиеся в конечном итоге к задачам на натуральные числа, решаются автоматически с помощью машин другого типа, а именно с помощью так называемых счётно-аналитических машин (сокращённо САМ). В их проектировании, производстве и использовании у нас за последние годы сделано особенно много: имеется завод САМ, их выпускающий, имеются «счётные фабрики» и «счётные станции», их использующие.

Рассмотрим два примера применения счётно-аналитических машин.

---

[1]) Н. А. Кобринский и Л. А. Люстерник, Математическая техника, Успехи математических наук, т. I, вып. 5—6 (15—16) (Новая серия), 1946.

Положим, имеется материал, собранный при переписи населения, в виде огромного числа карточек, содержащих данные о каждом переписанном лице, а именно данные о его поле, возрасте, национальности, образовании, профессии и т. д. Материал этот надо обработать, т. е. установить, сколько в отдельности мужчин и женщин, сколько человек в каждой возрастной группе и пр. Ручная раскладка карточек и подсчёт их по группам в силу их многочисленности требует непомерно большой затраты времени и даёт результаты, далеко не свободные от случайных ошибок. Естественно, что построены машины, производящие эти подсчёты автоматически с весьма большой скоростью. Все данные, полученные в результате переписи для каждого человека, переносятся на особую «перфорационную карту» (перфокарту), на которой каждому признаку соответствует одно сквозное отверстие (или группа отверстий). Эти перфокарты пропускаются с огромной скоростью через счётно-аналитическую машину, работающую от мотора и безошибочно подсчитывающую, сколько прошло карточек, имеющих отверстия на некотором определённом месте, т. е. сколько человек, имеющих некоторый определённый признак, зарегистрировано переписью.

В качестве второго примера возьмём «таблицу разностей», составляемую часто при решении различных задач, в которых данными являются значения некоторой функции. Ниже приведена такая таблица разностей первого, второго и третьего порядков для функции $f(x)=10^4\sqrt{x}$, заданной таблицей значений, округлённых до целых и соответствующих значениям аргумента x от 10 до 20 через 1.

x	$f(x)=10^4\sqrt{x}$	$\Delta f(x)$	$\Delta^2 f(x)$	$\Delta^3 f(x)$
10	31 623			
		1543		
11	33 166		—68	
		1475		8
12	34 641		—60	
		1415		6
13	36 056		—54	
		1361		6
14	37 417		—48	
		1313		5
15	38 730		—43	
		1270		4
16	40 000		—39	
		1231		3
17	41 231		—36	
		1195		4
18	42 426		—32	
		1163		1
19	43 589		—31	
		1132		
20	44 721			

Числа, записанные в столбце $\Delta f(x)$ и называемые «первыми разностями» или «разностями первого порядка», представляют собой разности двух соседних значений функций (из последующего вычитается предыдущее). Так, $33166 - 31623 = 1543$; $34641 - 33166 = 1475$ и т. д. Поступая точно так же со столбцом первых разностей, получим столбец вторых разностей, потом третьих, четвёртых и т. д. Нередко составление таблицы разностей приходится вести до разностей V, VI, VII и более высокого порядка. Это — работа, весьма простая по принципиальной своей стороне, но очень трудоёмкая и нуждающаяся в тщательной проверке каждого шага.

Несколько лет назад советский специалист по счётно-решающим устройствам И. Н. Янжул приспособил одну из счётно-аналитических машин, а именно так называемый «табулятор», к автоматическому выполнению этой операции составления разностной схемы. Для каждого значения данной функции изготовляется перфокарта; все перфокарты закладываются в машину, которая работает автоматически и печатает таблицу разностей. Если учесть все вспомогательные операции, связанные с работой автомата, то окажется, что этот способ даёт около 2000 значений разностей в час, причём каждая разность может иметь до 7 цифр. Это в 3—4 раза превосходит рекордную скорость такой работы, достигнутую за рубежом.

Разные счётно-аналитические машины (табуляторы, мультиплейеры и другие) позволяют очень быстро и очень точно составлять всевозможные таблицы. Данные задаются на перфокартах, машина работает автоматически от мотора и выбрасывает готовую таблицу в печатном виде.

Об истории счётно-аналитических машин и успехах, достигнутых в СССР в деле их проектирования, производства и использования, можно прочесть в статьях, напечатанных в журнале «Успехи математических наук» за 1946 и 1947 гг. Обширная библиография по вопросу механизации вычислений вообще дана в русском переводе книги Виллерс, Математические инструменты, вышедшей в 1949 г.

Отметим ещё специальную машину для решения системы уравнений первой степени. Решение любой такой системы не требует ничего, кроме четырёх арифметических действий над данными коэффициентами; принципиальная сторона всей работы доступна ученику VII класса, но когда неизвестных и уравнений много (бывают практические задачи, требующие решения систем с несколькими десятками неизвестных) и когда коэффициенты — числа многозначные, то решение систем становится делом, требующим многих месяцев напряжённой работы. Построено много машин, выполняющих эту работу несравненно быстрее, чем ручным способом. Отметим машину, построенную в 1940 г. советским изобретателем В. М. Прошко [1]). Она

[1]) В. М. Прошко, Приборы для определения корней системы линейных уравнений, Успехи математических наук, т. I, вып. 5—6 (15—16) (Новая серия), 1946.

позволяет автоматически решать систему из 10 уравнений первой степени с десятью неизвестными и с трёхзначными коэффициентами.

Работа по дальнейшему усовершенствованию существующих счётных машин, по созданию новых их типов ведётся у нас с успехом в ряде научных центров, из которых на первое место надо поставить Отдел приближённых вычислений Математического института Академии наук СССР. С этой работой можно детально ознакомиться по статье К. А. Семендяева в сборнике «Математика в СССР за тридцать лет», выпущенном Государственным издательством технико-теоретической литературы в 1948 г.

§ 5. Приближённые значения

Желая найти из опыта значение какой-либо неизвестной величины x, мы обращаемся к счёту или измерению, но получаем, как уже отмечалось выше, точное значение x лишь в исключительно редких простейших случаях и вынуждены довольствоваться его приближённым значением a: вместо точного равенства $x = a$ получаем равенство приближённое $x \approx a$. Школьная математика склонна игнорировать этот приближённый характер большинства чисел, с которыми мы имеем дело на практике, но не может обойти то обстоятельство, что уже в пятом классе при изучении десятичных дробей встречается деление, приводящее к бесконечным десятичным дробям, которые по необходимости приходится округлять, чтобы использовать их на практике или сделать возможными дальнейшие операции над ними. Таким образом, уже при изучении рациональных чисел школьная математика встречается с необходимостью рассматривать приближённые значения. В дальнейшем появляются различные иррациональные числа — корни, логарифмы, антилогарифмы, число π, значения тригонометрических и обратных круговых функций и т. д., и отсутствие в школьных программах специального раздела, посвящённого приближённым вычислениям, является серьёзным дефектом этих программ, весьма неблагоприятно сказывающимся на математической культуре молодёжи, оканчивающей среднюю школу.

Вот типичный случай из практики лаборатории физики. Требуется найти, по возможности точнее, среднюю плотность δ материала, из которого сделан кусок проволоки. Имея в своём распоряжении мерку Пальмера («толщемер»), миллиметровую линейку и лабораторные весы, устанавливаем, что диаметр проволоки равен $2r \approx 0{,}48$ *мм*, её длина $h \approx 264{,}4$ *мм*, её вес $p \approx 0{,}423$ *г*. Остаётся провести вычисление по формулам $\delta = \frac{p}{v}$, $v = \pi r^2 h$, где p должно быть выражено в граммах, r и h — в сантиметрах.

При вычислении встречаем ряд затруднений. Во-первых, с какой точностью взять π? Желая согласно заданию найти δ с наибольшей

возможной точностью, берём более точное значение 3,14159, приводимое обычно в учебниках, хотя остаётся сомнение, не лучше ли взять ещё больше знаков. Далее, находим:

$$r \approx 0{,}24 \text{ мм}, \quad r^2 \approx 0{,}0576 \text{ мм}^2, \quad \pi r^2 \approx 0{,}180955584 \text{ мм}^2,$$

$$v = 47{,}8246564096 \text{ мм}^3 = 0{,}0478246564096 \text{ см}^3.$$

Возникает второе затруднение: у получаемых чисел много десятичных знаков; не округлить ли их? Никаких указаний о том, какое округление в данном случае допустимо, обычный школьный курс математики не даёт, поэтому никакого округления из осторожности не делаем. Теперь при делении $p \approx 0{,}423$ *г* на найденное значение v мы встречаемся с третьим затруднением: сколько цифр взять в частном, которое выражается бесконечной десятичной дробью? Деление можно продолжать без конца, но ясно, что при взятых нами приближённых значениях r, h, p искомое значение δ можно получить тоже только приближённо. Здесь необходимо остановиться после получения какого-то числа десятичных знаков частного; игнорировать приближённый характер данных уже нельзя, но отсутствие определённых оснований для определения этого числа десятичных знаков создаёт тягостное состояние неуверенности, совершенно не вяжущееся с убеждением, что мы занимаемся применением точной науки — математики. Остановившись, например, после получения цифры сотых и замечая, что остаток от деления составляет больше половины частного, получаем, округляя частное до сотых по избытку, что $\delta \approx 8{,}84$, но не имеем никаких оснований утверждать ни того, что все цифры этого числа точны, ни того, что отброшенные нами цифры (тысячные и дальше) действительно не заслуживают доверия.

Весьма простые, вполне доступные уже пятиклассникам правила округления результатов действий над приближёнными значениями («правила подсчёта цифр») полностью устраняют все затруднения при вычислениях, аналогичные трём указанным, и значительно упрощают выкладки. О них будет итти речь ниже, в §§ 10—13. Применяя эти правила к решению только что рассмотренной задачи, мы придём к заключению, что $\delta \approx 8{,}8$ с уверенностью, что в цифре десятых сколько-нибудь значительная ошибка весьма мало вероятна, а отброшенные цифры (сотых, тысячных и т. д.) никакого доверия не заслуживают. Применяя несколько более громоздкий, но по идейной своей стороне более простой, вполне доступный учащимся семилетней школы «способ границ», мы устанавливаем, что, считая $0{,}475 < 2r < 0{,}485$ *мм*, $264{,}3 < h < 264{,}5$ *мм*, $0{,}422 < p < 0{,}424$ *г*, можно с абсолютной уверенностью утверждать, что искомая плотность δ заключается между 8,63 и 9,05, а потому $\delta \approx 8{,}8$ ($\pm 0{,}25$), т. е., что приближённое значение δ равно 8,8 и отличается от точного его значения во всяком случае меньше чем на 0,25 (выкладки проведены на стр. 390).

Из обычного курса арифметики учащиеся выносят умение округлять десятичные дроби до определённого разряда или, что то же, до определённого десятичного знака. Эта операция рассматривается в связи с действием деления[1]), но имеет значение и независимо от него. Округление данного десятичного числа, целого или дробного, до некоторого его разряда состоит в отбрасывании всех его цифр, находящихся правее цифры этого разряда. Если первая из отброшенных цифр есть 0, 1, 2, 3, 4, то полученное округлённое значение меньше данного, округление делается «по недостатку»; если же эта цифра есть 5, 6, 7, 8, 9, то последняя сохраняемая цифра усиливается (увеличивается на 1), округление делается «по избытку». В обоих случаях абсолютное значение разности между данным и округлённым числами («погрешность округления») не достигает половины единицы того разряда, до которого произведено округление; исключением является тот случай, когда округление состоит в отбрасывании одной лишь цифры 5, когда эта разность составляет ровно половину единицы последнего сохранённого разряда; тогда нередко применяется «правило чётной цифры»: округление делается по недостатку, если последняя сохраняемая цифра чётная, и по избытку, если она нечётная. Так, округление числа 345,0715 до сотен, десятков, единиц, десятых, сотых, тысячных даёт соответственно 300; 350; 345; 345,1; 345,07; 345,072; округление до тысячных числа 345,0725 даёт тоже 345,072.

Чтобы не возвращаться в дальнейшем к вопросу об округлении, заметим, что наряду с округлением до определённого разряда или, что то же, до определённого десятичного знака, применяется округление до определённого числа «значащих цифр». *Значащими цифрами* числа называются все его цифры, кроме нулей слева и тех нулей справа, которые заменяют отброшенные или неизвестные цифры. Так в числе 3,14 — два десятичных знака, но три значащие цифры. Округление числа 345,0715 до одной, двух, трёх, четырёх, пяти, шести значащих цифр даёт те же самые числа, что указаны выше. Округляя число 7893 до одной, двух, трёх значащих цифр, получаем соответственно 8000, 7900, 7890, где нули справа поставлены взамен неизвестных цифр и не являются значащими цифрами (лучше было бы писать 8???, 79??, 789?); число 37,0, выражающее, например, температуру, определённую с помощью медицинского термометра (со шкалой, разделённой на десятые доли градуса), имеет три значащие цифры; здесь цифра нуль справа является значащей.

Есть основания не считать значащей цифрой единицу, если она является цифрой старшего разряда приближённого числа, т. е. первой слева его цифрой (об этом будет речь на стр. 382). Принимая это правило, мы должны, например, число 12,47 считать имеющим не 4, а только 3 значащие цифры.

---

[1]) См. А. П. Киселёв, Арифметика, 1946, § 169 и 170.

§ 6. Различные способы оценки точности приближённых значений

Имея дело с приближёнными равенствами вида $x \approx a$, мы должны, прежде всего, выяснить точный их смысл. Что, в самом деле, означает выражение «икс приближённо равен такому-то числу»?

Приближённое равенство $x \approx a$ получает совершенно определённый смысл, если оно сопровождается указанием *границы абсолютной погрешности*, т. е. такого числа $\Delta a > 0$, прибавление которого даёт число $a + \Delta a$, заведомо большее истинного (неизвестного нам) значения x, или так называемую *высшую границу* x (ВГ x), а вычитание — число $a - \Delta a$, заведомо меньшее x, или так называемую *низшую границу* x (НГ x). Так, например, равенство $x \approx 27{,}4\ (\pm 0{,}1)$ *кг* означает, что $27{,}4 - 0{,}1 = 27{,}3$ *кг* меньше x, а $27{,}4 + 0{,}1 = 27{,}5$ *кг* больше x. Общепринятая запись $x \approx a\ (\pm \Delta a)$ равносильна, таким образом, двойному неравенству $a - \Delta a < x < a + \Delta a$. Обратно, зная НГ x и ВГ x, т. е. имея двойное неравенство вида $p < x < q$, легко находим приближённое значение $a = \frac{q+p}{2}$ и границу абсолютной погрешности $\Delta a = \frac{q-p}{2}$.

Приближённое равенство $x \approx a\ (\pm \Delta a)$ означает следующее: «икс приближённо равен a с границей абсолютной погрешности, равной Δa» или «икс приближённо равен a, отличаясь от a в ту или другую сторону меньше чем на Δa».

В некоторых случаях строгое неравенство $a - \Delta a < x < a + \Delta a$ заменяется неравенством более общего вида $a - \Delta a \leqslant x \leqslant a + \Delta a$.

Согласно твёрдо установившейся со времён Гаусса традиции все приближённые числа, приводимые в математических таблицах, имеют границы абсолютной погрешности, равные половине единицы последнего имеющегося в них разряда. Например, найдя в таблице логарифмов $\lg 7 \approx 0{,}8451$, мы можем быть уверены, что истинное значение $\lg 7$ отличается от 0,8451 меньше чем на $0{,}0001 : 2 = 0{,}00005$, и что, следовательно, $0{,}84505 < \lg 7 < 0{,}84515$. Точно так же, найдя в таблице $\operatorname{tg} 89°59' \approx 3438$, мы можем быть уверены, что $3437{,}5 < \operatorname{tg} 89°59' < 3438{,}5$.

Возможно и употребительно другое определение границы абсолютной погрешности, совершенно равносильное указанному выше. Полагая $x = a + \xi$, называют число $\xi = x - a$ (оно неизвестно, если неизвестно x) *абсолютной погрешностью* или просто *погрешностью* приближённого числа a, а *границей* абсолютной погрешности этого приближённого числа называют любое число $\Delta a > 0$, удовлетворяющее неравенству $|\xi| < \Delta a$ или $|x - a| < \Delta a$ или, что то же, двойному неравенству $-\Delta a < x - a < \Delta a$. Прибавляя a ко всем трём частям этого последнего неравенства, получим неравенство $a - \Delta a < x < a + \Delta a$, которым пользовались для первого опреде-

ления границы абсолютной погрешности. Возможность обратного перехода от этого последнего неравенства к неравенству $|x-a|<\Delta a$ показывает полную равносильность этих двух определений.

Указание границы абсолютной погрешности позволяет сравнивать точность различных приближений одного и того же неизвестного значения: чем меньше Δa, тем точнее приближённое значение a. Если, например, один раз найдено, что $x\approx 5{,}64\ (\pm 0{,}01)$, а другой раз, что $x\approx 5{,}63183\ (\pm 0{,}00002)$, то можно сказать, что второе приближение точнее первого в $0{,}01:0{,}00002=500$ раз. Но для сравнения точности приближений к различным числам указание их границы абсолютной погрешности само по себе уже недостаточно. Пусть, например, известно, что два измерения длины выполнены с одной и той же границей абсолютной погрешности, равной 1 *мм*, причём в одном случае измерялся диаметр проволоки, оказавшийся приближённо равным 2 *мм*, а в другом — геодезический базис, близкий к 1 *км*. Ясно, что первое измерение сделано очень грубо, граница абсолютной погрешности составляет целых 50% приближённого значения, второе же весьма точно, так как граница абсолютной погрешности составляет только $0{,}0001\%$ полученного числа. Таким образом, приходим к понятию *границы относительной погрешности*, определяемой как отношение границы абсолютной погрешности к приближённому значению, т. е. $\frac{\Delta a}{a}$ (или к неизвестному точному значению, т. е. $\frac{\Delta a}{x}$, что практически сводится к тому же), и выражаемой обычно в процентах. Указание границы относительной погрешности весьма распространено на практике. Так различные радиодетали (сопротивления, конденсаторы, катушки самоиндукции и др.) обычно имеют надписи вроде такой: «200 *ом* $\pm 10\%$», означающей, что данное сопротивление отличается от 200 *ом* не более чем на 10% этой величины, т. е. на 20 *ом*, и содержится в границах от 180 до 220 *ом*.

Отметим, что граница относительной погрешности приближённого числа не меняется при переходе к другой единице измерения, в частности, остаётся неизменной при переносе знака дробности, так как при этом в одно и то же число раз увеличивается или уменьшается и a и Δa.

Указание границы абсолютной или относительной погрешности представляет собой два основных способа характеристики точности приближённых чисел.

На практике оба эти способа применяются сравнительно редко. Несравненно чаще точность приближённого числа характеризуется простым указанием на число его цифр, заслуживающих доверия. Если граница абсолютной погрешности приближённого числа равна полуединице разряда последней его цифры, говорят, что все цифры этого числа точны. Таким образом, приближённое

число, все цифры которого точны, представляет собой результат округления до некоторого разряда соответствующего истинного неизвестного нам числа; таковы все числа, приводимые в математических таблицах. Указывая число значащих цифр такого приближённого числа, тем самым характеризуют его точность. Двузначным, трёхзначным, вообще k-значным приближённым числом следует считать в соответствии с этим приближённое число, имеющее 2, 3, вообще k точных значащих цифр. Этот способ характеристики точности приближённых чисел имеет то достоинство, что не требует никаких дополнительных указаний: запись числа говорит сама за себя.

Указание числа точных цифр и места знака дробности равносильно указанию границы абсолютной погрешности; так, четырёхзначные квадратные корни из чисел от 1 до 100, в которых знак дробности стоит после первой значащей цифры, имеют границу абсолютной погрешности, равную 0,0005. Вместе с тем возможно и некоторое заключение о границе относительной погрешности, хотя и менее определённое, чем о границе абсолютной погрешности, но тем не менее весьма существенное для обоснования некоторых практических правил. Действительно, пусть дано k-значное приближённое число, все цифры которого точны, и пусть знак дробности поставлен после последней его цифры (как мы уже знаем, перенос запятой относительной погрешности не меняет). Это число a удовлетворяет неравенству $10^{k-1} < a < 10^k$, причём $\Delta a = 0{,}5$, а потому граница относительной погрешности заключена между $0{,}5 \cdot 10^{-k}$ и $0{,}5 \cdot 10^{-(k-1)}$. Выражая её в процентах, получаем следующую таблицу:

k	2	3	4	5	6
$\frac{\Delta a}{a}$	от 0,5 до 5%	от 0,05 до 0,5%	от 0,005 до 0,05%	от 0,0005 до 0,005%	от 0,00005 до 0,0005%

Если не считать значащей цифрой единицу, когда она является цифрой старшего разряда приближённого числа, то границы значений $\frac{\Delta a}{a}$ в этой таблице уменьшаются вдвое, так как при соблюдении этого условия имеем неравенство $2 \cdot 10^{k-1} < a < 2 \cdot 10^k$.

Нередко даётся несколько иное, чем выше, определение понятия «точные цифры». Так, в статье П. С. Александрова и А. Н. Колмогорова [6] читаем: «говорят, что какая-либо цифра данного приближённого значения числа точная, если погрешность не превосходит по абсолютной величине единицы соответствующего разряда». На практике на каждом шагу встречаются приближённые числа, в которых погрешность (абсолютная) может быть ещё больше; так, уже сложение четырёх слагаемых, каждое из которых имеет погрешность не более половины сотой, приводит к сумме, погрешность

которой может быть близкой к двум сотым. Если вероятность больших значений погрешности в последней цифре приближённого числа много меньше, чем малых её значений, то эту цифру всё же сохраняют, как заслуживающую в известной мере доверия, хотя и без гарантии, что она точная. В дальнейшем мы будем иметь много примеров таких чисел.

Итак, мы ознакомились с тремя способами характеристики точности приближённых чисел: посредством указания границ их абсолютных погрешностей, посредством указания границ их относительных погрешностей, посредством указания числа их цифр, заслуживающих доверия. Именно этот последний способ и употребляется чаще всего на практике. В дальнейшем мы встретимся ещё с двумя способами, имеющими большое теоретическое значение, но вовсе неприменяемыми в средней школе, а именно, характеристикой точности приближённого числа через указание средней квадратической его погрешности и с указанием вероятности различных значений его погрешности.

§ 7. Обработка результатов измерений

В простейших случаях, с какими чаще всего и приходится иметь дело в школе, измерение даёт приближённый результат, точность которого легко характеризуется указанием его границы абсолютной погрешности. Так, измеряя миллиметровой линейкой длину x карандаша и замечая, что она заключается между 178 и 179 *мм*, ближе к 179, заключаем, что $x \approx 179\ (\pm 0{,}5)$ *мм* или, стремясь уменьшить границу абсолютной погрешности, что $x \approx 178{,}75\ (\pm 0{,}25)$ *мм*. При всяком взвешивании легко устанавливают, при какой наибольшей нагрузке чашки с гирями перетягивает чашка с грузом и какая минимальная добавка гирь вызывает перевес чашки с гирями. Если, например, мы пользуемся разновесом до 0,1 *г* и замечаем, что при нагрузке в 67,6 *г* перетягивает груз, а при нагрузке в 67,7 *г* перетягивают гири, то тем самым определяются низшая и высшая границы искомого веса, а отсюда и приближённое его значение, равное $(67{,}6 + 67{,}7) : 2 = 67{,}65$ *г*, и граница абсолютной его погрешности, равная $(67{,}7 - 67{,}6) : 2 = 0{,}05$ *г*.

Стремясь обеспечить наибольшую возможную в данных условиях точность измерения, делят на-глаз на 5 или 10 равных частей то наименьшее деление, какое имеется на шкале применяемого измерительного прибора, и находят лишний десятичный знак искомого значения посредством глазомерной оценки. При этом каждое повторное измерение даёт обычно результат, уже несколько отличный от предшествующего: сказываются и ошибки этой глазомерной оценки, и неточность установки (например, нулевая точка масштабной линейки при каждом новом её прикладывании может оказаться сдви-

нутой на небольшую долю миллиметров относительно начальной точки измеряемого отрезка), и неполная определённость самого измеряемого объекта; так, при измерении длины отрезка его концы обычно отмечаются тонкими поперечными штрихами, имеющими толщину примерно в 0,1 *мм*, и приходится на-глаз искать их середины. Это колебание результата измерения в более сложных случаях весьма усиливается. Так бывает, например, если на местности измеряется длинный отрезок, в котором применяемый измеритель (20-метровая лента) укладывается несколько раз, или если хотят найти средний вес сотни зёрен пшеницы, взятых наудачу из некоторой её партии.

Получив в результате повторных измерений несколько более или менее близких друг к другу приближённых значений $a_1, a_2, a_3, \ldots, a_n$ одной и той же неизвестной величины x, мы должны произвести обработку этих результатов с целью получения, во-первых, наиболее близкого к x значения a и, во-вторых, характеристики точности приближённого равенства $x \approx a$.

Нередко бывает, что все полученные измерением значения имеют некоторую систематическую погрешность, обусловленную постоянно действующей причиной. Так, пользуясь миллиметровой линейкой, деления которой несколько короче нормальных, мы постоянно будем получать преувеличенные результаты, а взвешивая деревянный предмет с помощью латунного разновеса, получим значения, меньшие истинного из-за потери в весе от вытесненного воздуха (закон Архимеда в газах). Такого рода погрешности должны быть учтены и устранены введением надлежащих поправок. Так, установив, что 100 делений нашей масштабной линейки равны не 100 *мм*, а лишь 98,5 *мм*, мы должны полученные в делениях нашего масштаба результаты умножить на 0,985, чтобы выразить эти результаты в миллиметрах.

После устранения таких систематических погрешностей остаются погрешности случайные, вызывающие расхождение результатов отдельных измерений. Если все значения $a_1, a_2, \ldots, a_n$ получены при одних и тех же условиях и заслуживают одинакового доверия, в качестве вероятнейшего значения искомой величины x берут их среднее арифметическое $a = (a_1 + a_2 + \ldots + a_n) : n$ или, применяя более удобную запись, $a = \left(\sum_{i=1}^{n} a_i\right) : n$. Значения a_i отнюдь не обязательно различны. Если a_1 повторяется n_1 раз, a_2 — n_2 раз, вообще a_i — n_i раз, то для определения среднего арифметического удобнее пользоваться формулой

$$a = \left(\sum_{i=1}^{k} a_i n_i\right) : n,$$

где $n = n_1 + n_2 + \ldots + n_k$.

Этот весьма распространённый на практике способ вполне оправдывается теоретическими соображениями [1]), хотя наряду с ним употребляются и некоторые другие способы; например, располагают полученные значения в порядке возрастания и берут *среднее* значение, т. е. значение, одинаково удалённое от концов ряда («медиану»).

Приняв $x \approx a$, $a = (a_1 + a_2 + \ldots + a_n) : n$, мы должны выяснить, какова точность этого приближённого равенства. В школе эту оценку производят путём простого сравнения числа a с результатами отдельных измерений a_1, a_2, ..., a_n. Среднее a округляют, сохраняя все цифры, остающиеся неизменными или почти неизменными во всех значениях a_i, и отбрасывая все последующие.

Можно рекомендовать вычисление *отклонений от среднего*, т. е. разностей $a - a_i$. Сумма этих разностей, как легко видеть, равна нулю (контроль!). Среднее из абсолютных значений этих разностей («среднее отклонение») можно считать характеристикой точности найденного среднего. С некоторой определённой вероятностью, подсчитываемой рассмотренным дальше способом, можно утверждать, что истинное значение x отличается от a меньше, чем на это среднее отклонение.

Пример. Пусть неизвестная величина измерена пять раз; результаты измерений приведены во втором столбце следующей таблицы:

i	a_i	$a - a_i$	$(a - a_i)^2$
1	4,781	+ 0,0022	0,00000 484
2	4,795	— 0,0118	13 924
3	4,769	+ 0,0142	20 164
4	4,792	— 0,0088	7 744
5	4,779	+ 0,0042	1 764
Сумма абсолютных значений	23,916	0,0412	0,00044080
Среднее a	4,7832	0,00824	

Какие цифры найденного среднего $a = 4{,}7832$ следует сохранить? Цифры целых (4) и десятых (7) повторяются во всех результатах отдельных измерений и безусловно надёжны. Цифры сотых колеблются, но весьма незначительно (от 6 до 9), поэтому третья цифра среднего (цифра сотых 8) тоже заслуживает доверия и подлежит сохранению. Возникает вопрос о цифре тысячных (3). Она

[1]) См. Э. э. м., кн. 6, Б. В. Гнеденко, Элементы теории вероятностей и математической статистики.

весьма ненадёжна и может быть отброшена, но обычно всё же такую первую сомнительную цифру предпочитают сохранять (уже из стремления сделать незаметной вводимую погрешность округления). Цифры же, расположенные правее этой первой сомнительной цифры, в данном случае цифра десятитысячных (2), подлежат отбрасыванию. Итак, в данном случае $x \approx a = 4{,}783$. Мы получили приближённое число с четырьмя значащими цифрами (с тремя десятичными знаками), причём первые три значащие цифры надёжны, четвёртая сомнительна. Этот же вывод подтверждается и вычислением среднего отклонения. Найдя отклонения от среднего, приведённые в третьем столбце таблички, подсчитываем отдельно положительные отклонения (сумма $+0{,}0206$) и отрицательные отклонения (сумма $-0{,}0206$), а потому сумма всех отклонений нуль, как и должно быть; сумма абсолютных значений отклонений равна $0{,}0206 \cdot 2 = 0{,}0412$, среднее отклонение $0{,}0412 : 5 = 0{,}00824$ или после округления до одной значащей цифры 0,008. Этот результат можно считать подтверждением сделанного выше заключения о надёжности цифры сотых и сомнительности цифры тысячных.

Такого рода оценкой точности среднего арифметического и приходится ограничиваться в школьной практике. Более точный, вполне обоснованный в теории ошибок способ обработки результатов равноточных измерений заключается в следующем (приводим только указания о практическом применении этого способа, отсылая желающих ознакомиться с его теорией к книге [7]; для понимания этой книги и нужны некоторые сведения из теории вероятностей, которые можно взять из книги [8] [1]).

Найдя среднее значение $a = \frac{\Sigma a_i}{n}$ и отклонения от среднего $a - a_i$, берут квадраты этих отклонений и вычисляют «среднее квадратическое отклонение» s по формуле $s^2 = \frac{\Sigma (a - a_i)^2}{n - 1}$; это число s является характеристикой точности всего использованного ряда измерений. Далее, по формуле $s_a = s : \sqrt{n}$ находят «среднее квадратическое отклонение арифметического среднего». Вероятность α неравенства $a - \varepsilon < x < a + \varepsilon$, т. е. вероятность того, что искомое значение x отличается от найденного среднего значения a меньше, чем на некоторое произвольное число ε (в ту или другую сторону), зависит от отношения $t = \varepsilon : s_a$ и от числа измерений n (или, что то же, от числа $k = n - 1$) и выражается довольно сложной формулой, для которой составлена таблица, позволяющая по данным значениям $k = n - 1$ и t находить α, а также по данным k и α находить t, а следовательно, и ε. Приводим отрывок этой таблицы, заимствованный из книги [7].

---

[1]) См. также Э. э. м., кн. 6, Б. В. Гнеденко, Элементы теории вероятностей и математической статистики.

$k=n-1$	$t=2{,}0$	$t=2{,}5$	$t=3{,}0$	$t=3{,}5$	$k=n-1$	$t=2{,}0$	$t=2{,}5$	$t=3{,}0$	$t=3{,}5$
1	0,7048	0,7578	0,7952	0,8228	11	0,9292	0,9704	0,9880	0,9950
2	8164	8704	9046	9276	12	9314	9720	9890	9956
3	8606	9122	9424	9606	13	9332	9737	9898	9960
4	8838	9332	9600	9752	14	9348	9740	9904	9964
5	8980	9456	9700	9828	15	9360	9754	9910	9968
6	9076	9534	9760	9872	16	9372	9764	9916	9970
7	9144	9590	9800	9900	17	9382	9770	9920	9972
8	9194	9630	9830	9920	18	9392	9776	9924	9974
9	9234	9662	9850	9932	19	9400	9782	9926	9976
10	9266	9686	9865	9942	20	9108	9788	9930	9978
					∞	9545	9876	9973	9995

Возвращаясь к рассмотренному выше примеру, имеем $n=5$, $k=4$, $a=4{,}7832$, $s^2=0{,}00044080:4=0{,}00011020$, $s=0{,}0105$, $s_a=0{,}0105:\sqrt{5}=0{,}0021\cdot\sqrt{5}=0{,}00469$. Найдём, при каком значении ε вероятность неравенства $a-\varepsilon<x<a+\varepsilon$ равна 0,96. Таблица показывает, что при $k=4$ вероятность $\alpha=0{,}96$, если $t=3{,}0$, а потому $\varepsilon=t\cdot s_a=3{,}0\cdot 0{,}00469\approx 0{,}0141$. Итак, с вероятностью в 0,96 можно утверждать, что истинное значение x отличается от найденного среднего $a=4{,}7832$ меньше, чем на $\varepsilon=0{,}0141$. Другими словами, 96 из каждых ста шансов за то, что x отличается от $a=4{,}7832$ меньше, чем на $\varepsilon=0{,}0141$, и только четыре против. Как видно из таблицы, чем больше число измерений n, тем больше при постоянном t и вероятность α, а при одном и том же числе измерений n эта вероятность α растёт с ростом $t=\varepsilon:s_a$, т. е. с ростом ε и убыванием s_a.

Посмотрим ещё, как велика вероятность того, что истинное значение x отличается от среднего $a=4{,}7832$ меньше, чем на величину найденного среднего отклонения 0,00824. Теперь $\varepsilon=0{,}00824$, $t=0{,}00824:0{,}00469=1{,}76$. Таблица показывает, что здесь α несколько меньше, чем 0,8838; можно считать, что $\alpha\approx 0{,}85$.

В заключение настоящего параграфа отметим, что наибольшее значение для школы имеет тот простейший способ оценки точности результатов однократных измерений, о котором шла речь в его начале. Если учащиеся средней школы будут приучены при проведении каждого измерения указывать границу абсолютной погрешности результата или, что сводится к тому же, устанавливать низшую и высшую границы искомого неизвестного числа, то тем самым будет сделан существенный шаг вперёд в деле устранения формального усвоения школьной математики.

ГЛАВА II

УЧЁТ ПОГРЕШНОСТЕЙ

§ 8. Вычисления со строгим учётом погрешностей по способу границ

Производя какое-нибудь вычисление с приближёнными данными, мы получаем результат, по необходимости тоже приближённый. На нём не могут не сказаться как погрешности данных, так и «вычислительные погрешности», обусловленные неизбежными округлениями, производимыми в ходе вычисления. Возникает вопрос первостепенной важности: как оценить точность результата такого вычисления с приближёнными данными?

Наилучший в смысле строгости и доступности способ такого «учёта погрешностей» в результатах вычислений представляет собой способ границ. Зная низшую и высшую границы (НГ и ВГ) каждого из данных, без особого труда (по крайней мере в более простых случаях) устанавливают НГ и ВГ результата каждого действия над этими данными и в конце концов получают НГ и ВГ искомого окончательного результата. Именно этот способ применил Архимед в своей знаменитой работе «Измерение круга». Он не ограничился получением приближённого значения отношения окружности к диаметру, равным 22:7, а показал, что это отношение, обозначаемое теперь буквой π, больше чем $3\frac{10}{71}$ и меньше чем $3\frac{1}{7}$, т. е. установил, что НГ $\pi = 3\frac{10}{71}$, ВГ $\pi = 3\frac{1}{7}$.

«Архимед последовательно определяет стороны описанных 6-угольника, 12-угольника, 24-угольника, 48-угольника и 96-угольника, выраженные с помощью диаметра, а именно, с тонким математическим чутьём он даёт для определяемого лишь приближённо отношения диаметра к стороне описанного многоугольника всегда несколько меньшее значение для того, чтобы получить для его периметра и, тем более для длины окружности, верную верхнюю границу... Чтобы найти нижнюю границу отношения длины окружности к диаметру, Архимед пользовался соответствующими вписан-

ными многоугольниками. При этих вычислениях Архимед с той же сознательной уверенностью берёт встречающиеся квадратные корни всякий раз так, чтобы получить для соответствующих сторон многоугольника немного меньшие значения. Таким образом, он получает для периметра вписанного многоугольника, а следовательно, тем более для окружности, верную нижнюю границу» [1]).

Теоретическая сторона способа границ в высшей степени проста. Она сводится к использованию хорошо известных ещё с первых классов школы предложений об изменении результатов действий в зависимости от изменения компонентов. Ограничиваясь первыми четырьмя арифметическими действиями, имеем такие предложения о границах (неизвестные x и y предполагаются положительными):

$$\text{НГ}(x+y)=\text{НГ}\,x+\text{НГ}\,y, \quad \text{ВГ}(x+y)=\text{ВГ}\,x+\text{ВГ}\,y,$$
$$\text{НГ}(x-y)=\text{НГ}\,x-\text{ВГ}\,y, \quad \text{ВГ}(x-y)=\text{ВГ}\,x-\text{НГ}\,y,$$
$$\text{НГ}(xy)=\text{НГ}\,x\cdot\text{НГ}\,y, \quad \text{ВГ}(xy)=\text{ВГ}\,x\cdot\text{ВГ}\,y,$$
$$\text{НГ}\left(\frac{x}{y}\right)=\frac{\text{НГ}\,x}{\text{ВГ}\,y}, \quad \text{ВГ}\left(\frac{x}{y}\right)=\frac{\text{ВГ}\,x}{\text{НГ}\,y}.$$

Сюда надо присоединить ещё три предложения, вытекающих непосредственно из определений НГ и ВГ: 1) округлять НГ можно только по недостатку, ВГ — только по избытку; 2) чем меньше разность $\text{ВГ}\,x-\text{НГ}\,x$, тем точнее определяется x; 3) в качестве приближённого значения x рекомендуется брать среднее арифметическое чисел $\text{НГ}\,x$ и $\text{ВГ}\,x$ или число, близкое к этому среднему.

Простейшие применения способа границ не представляют никаких затруднений и вполне разъясняются следующим примером.

Пример 1. Найти $x=\dfrac{a+b}{(a-b)c}$ при $a=3\frac{4}{7}$, $b=3\frac{5}{11}$, $c=28\frac{1}{3}$, заменяя точные значения a, b, c их приближёнными значениями, взятыми с точностью до сотых долей.

Решение.

	НГ	ВГ
a	3,57	3,58
b	3,45	3,46
$a+b=m$	7,02	7,04
$a-b$	0,11	0,13
c	28,33	28,34
$(a-b)c=n$	3,11	3,69
$x=\dfrac{m}{n}$	1,90	2,27

$$\begin{array}{rr} +\,2{,}27 & -\,2{,}27 \\ \underline{+\,1{,}90} & \underline{-\,1{,}90} \\ 4{,}17:2=2{,}085 & 0{,}37:2=0{,}185 \end{array}$$

$$x\approx 2{,}085\ (\pm 0{,}185)$$
$$x\approx 2{,}1\ \ (\pm 0{,}2)$$

[1]) Ф. Рудио, О квадратуре круга, перев. с нем., под ред. и с примеч. акад. С. Н. Бернштейна, ГТТИ, изд. 3-е, 1936, стр. 31—32.

Пояснение. Получив двойное неравенство $1{,}90 < x < 2{,}27$, естественно взять в качестве приближённого значения для x среднее между найденными границами, а именно, 2,085, но при этом может получиться впечатление, что мы нашли x с точностью до тысячных. Этого «очковтирательства» не будет, если одновременно указать, как велико наибольшее возможное отклонение истинного значения от этого среднего, т. е. указать *границу абсолютной погрешности* этого среднего, равную полуразности границ, и записать ответ в виде приближённого равенства $x \approx 2{,}085\ (\pm 0{,}185)$. Далее, округляем найденное значение так, чтобы в нём оставалась только одна сомнительная цифра. Взяв $x \approx 2{,}1$ и замечая, что $2{,}1 - 1{,}9 = 0{,}2$; $2{,}27 - 2{,}1 = 0{,}17$, имеем окончательно $x \approx 2{,}1\ (\pm 0{,}2)$.

В данном примере точные значения a, b, c нам известны, и мы можем сравнить полученный результат с точным значением x, равным $2\frac{31}{255} = 2{,}1215\ldots$ Как видим, это точное значение действительно содержится внутри указанных нами границ 1,90 и 2,27. Найденное нами приближённое значение 2,1 отличается от истинного очень немного: мы ручались, что оно отличается от истинного меньше, чем на 0,2, а в действительности разница едва превосходит 0,02. Таким образом, оценка погрешности оказалась преувеличенной; это наблюдается почти всегда.

Приводим полностью выкладки, нужные для решения примера, рассмотренного на стр. 378: найти $\delta = p : v$, $v = \pi r^2 h$, если $2r \approx 0{,}48\ (\pm 0{,}005)$ *мм*, $h \approx 264{,}4\ (\pm 0{,}1)$ *мм*, $p \approx 0{,}423\ (\pm 0{,}001)$ *г*; значения r и h надо выразить в сантиметрах.

Значения πr^2 взяты по таблице площади круга.

	НГ	ВГ
$2r$	0,0475	0,0485
πr^2	0,001772	0,001847
h	26,43	26,45
$v = \pi r^2 h$	0,0468	0,0489
p	0,422	0,424
$\delta = p : v$	8,63	9,05

$$\begin{array}{rr} +\ 9{,}05 & -\ 9{,}05 \\ \underline{\ \ 8{,}63} & \underline{\ \ 8{,}63} \\ 17{,}68 : 2 = 8{,}84 & 0{,}42 : 2 = 0{,}21 \end{array}$$

$\delta \approx 8{,}84\ (\pm 0{,}21)$,
$\delta \approx 8{,}8\ \ (\pm 0{,}25)$.

Рассмотрим более трудный пример, доступный учащимся IX и X классов.

Пример 2. Вычислить с четырьмя точными десятичными знаками значения $\sin 3°$ и $\cos 3°$, исходя из формул $a_6 = r$, $a_{10} = 0{,}5r(\sqrt{5} - 1)$, выражающих длины сторон правильных 6-угольника и 10-угольника, вписанных в круг радиуса r.

Решение.

$\sin 30^\circ = 0{,}5a_6 : r = 0{,}5$; $\cos 30^\circ = \sqrt{1 - 0{,}25} = 0{,}5\sqrt{3}$;

$\sin 18^\circ = 0{,}5a_{10} : r = 0{,}25(\sqrt{5} - 1)$; $\cos 18^\circ = 0{,}25\sqrt{10 + \sqrt{20}}$;

$\sin 15^\circ = \sqrt{0{,}5(1 - \cos 30^\circ)} = 0{,}5\sqrt{2 - \sqrt{3}} = 0{,}25(\sqrt{6} - \sqrt{2})$;

$\cos 15^\circ = \sqrt{0{,}5(1 + \cos 30^\circ)} = 0{,}5\sqrt{2 + \sqrt{3}} = 0{,}25(\sqrt{6} + \sqrt{2})$;

$\sin 3^\circ = \sin(18^\circ - 15^\circ) = \sin 18^\circ \cos 15^\circ - \cos 18^\circ \sin 15^\circ$;

$\cos 3^\circ = \cos 18^\circ \cos 15^\circ + \sin 18^\circ \sin 15^\circ$.

Вычисление.

$\sin 15^\circ = 0{,}25(\sqrt{6} - \sqrt{2})$, $\cos 15^\circ = 0{,}25(\sqrt{6} + \sqrt{2})$.

	НГ	ВГ
$\sqrt{6}$	2,44948	2,44950
$\sqrt{2}$	1,41420	1,41422
$a_1 = \sqrt{6} - \sqrt{2}$	1,03526	1,03530
$b_1 = \sqrt{6} + \sqrt{2}$	3,86368	3,86372
$\sin 15^\circ = a_1 : 4$	0,25881	0,25883
$\cos 15^\circ = b_1 : 4$	0,96592	0,96593

Результат (с четырьмя точными десятичными знаками):

$\sin 15^\circ \approx 0{,}2588$,

$\cos 15^\circ \approx 0{,}9659$.

Вычисление.

$\sin 18^\circ = 0{,}25(\sqrt{5} - 1)$, $\cos 18^\circ = 0{,}25\sqrt{10 + \sqrt{20}}$.

	НГ	ВГ
$\sqrt{5}$	2,23606	2,23608
$a_2 = \sqrt{5} - 1$	1,23606	1,23608
$\sin 18^\circ = a_2 : 4$	0,30901	0,30902
$\sqrt{20}$	4,47213	4,47215
$b_2 = 10 + \sqrt{20}$	14,47213	14,47215
$c_2 = \sqrt{b_2}$	3,80421	3,80424
$\cos 18^\circ = c_2 : 4$	0,95105	0,95106

Результат (с четырьмя точными десятичными знаками):

$\sin 18^\circ \approx 0{,}3090$,

$\cos 18^\circ \approx 0{,}9511$.

Вычисление.

$$\sin 3^\circ = \sin 18^\circ \cos 15^\circ - \cos 18^\circ \sin 15^\circ,$$
$$\cos 3^\circ = \cos 18^\circ \cos 15^\circ + \sin 18^\circ \sin 15^\circ.$$

	НГ	ВГ
$a_3 = \sin 18^\circ$ $b_3 = \cos 15^\circ$ $c_3 = \cos 18^\circ$ $d_3 = \sin 15^\circ$	0,30901 0,96592 0,95105 0,25881	0,30902 0,96593 0,95106 0,25883
a_3b_3	0,29847	0,29849
c_3d_3	0,24614	0,24616
$\sin 3^\circ = a_3b_3 - c_3d_3$	0,05231	0,05235
b_3c_3 a_3d_3	0,91853 0,07997	0,91865 0,07998
$\cos 3^\circ = b_3c_3 + a_3d_3$	0,99860	0,99863

Результат (с четырьмя десятичными знаками):

$$\sin 3^\circ \approx 0{,}0523,$$
$$\cos 3^\circ \approx 0{,}9986.$$

Для контроля можно было бы вычислить сумму $s = \sin^2 3^\circ + \cos^2 3^\circ$ и убедиться, что НГ $s < 1$, ВГ $s > 1$, как и должно быть, но проще навести справку в таблицах. По четырёхзначной таблице получаем как раз найденные у нас значения $\sin 3^\circ$ и $\cos 3^\circ$, а шестизначная таблица (Петерса) даёт: $\sin 3^\circ = 0{,}052336$, $\cos 3^\circ = 0{,}998630$, что вполне согласуется с нашими результатами. Отметим, что более точное значение $\cos 3^\circ$ есть 0,99862995.

§ 9. Вычисления со строгим учётом погрешностей по способу границ погрешностей

При всей своей строгости и доступности способ границ, требуя вычисления НГ и ВГ, оказывается весьма громоздким: все выкладки приходится повторять дважды. Естественно, возникает вопрос: нельзя ли указать такой способ вычисления со строгим учётом погрешностей, который давал бы возможность находить приближённое значение искомого числа и границу его погрешности в зависимости от приближённых значений данных и границ их погрешности без вычисления НГ x и ВГ x?

Пусть известно, что $x \approx a\,(\pm \Delta a)$ и $y \approx b\,(\pm \Delta b)$, и требуется найти приближённые значения чисел $x+y$, $x-y$, xy, $\frac{x}{y}$, x^n, $\sqrt[n]{x}$ (n — натуральное число), характеризуя их точность.

Из неравенств

$$a - \Delta a < x < a + \Delta a, \tag{1}$$

$$b - \Delta b < y < b + \Delta b \tag{2}$$

почленным сложением получаем неравенство

$$a + b - (\Delta a + \Delta b) < x + y < a + b + (\Delta a + \Delta b). \tag{3}$$

Если умножить все члены неравенства (2) на -1 и переписать его в виде

$$-b - \Delta b < -y < -b + \Delta b,$$

то почленное сложение его с (1) даёт неравенство

$$a - b - (\Delta a + \Delta b) < x - y < a - b + (\Delta a + \Delta b). \tag{4}$$

Объединяя неравенства (3) и (4), получаем следующую теорему:

Теорема I. *Граница абсолютной погрешности суммы и разности приближённых чисел равна сумме границ абсолютных погрешностей этих чисел.* Эта теорема обобщается на алгебраическую сумму с любым числом членов.

Предполагая все члены неравенств (1) и (2) положительными, почленно перемножаем эти неравенства и получаем:

$$ab - (a\,\Delta b + b\,\Delta a) + \Delta a\,\Delta b < xy < ab + (a\,\Delta b + b\,\Delta a) + \Delta a\,\Delta b. \tag{5}$$

Произведение $\Delta a\,\Delta b$ в левой части можно отбросить, усиливая это неравенство. Но, считая числа Δa и Δb значительно меньшими, чем a и b, как это обычно и бывает на практике, мы отбросим это произведение $\Delta a\,\Delta b$, представляющее собой число «второго порядка малости» по отношению к произведению ab, и в правой части неравенства, лишая тем самым рассматриваемый способ границ погрешностей того безупречно строгого характера, какой имеет изложенный выше способ границ. Получаем новое неравенство

$$ab - (a\,\Delta b + b\,\Delta a) < xy < ab + (a\,\Delta b + b\,\Delta a), \tag{6}$$

или после понятных преобразований

$$-\left(\frac{\Delta a}{a} + \frac{\Delta b}{b}\right) < \frac{xy - ab}{ab} < \frac{\Delta a}{a} + \frac{\Delta b}{b}. \tag{7}$$

Последнее неравенство выражает новую теорему.

Теорема II. *Граница относительной погрешности произведения равна сумме границ относительных погрешностей сомножителей.*

Чтобы придти к аналогичной теореме о частном, найдём предварительно, чему равна граница относительной погрешности числа $1:b$ в зависимости от границы относительной погрешности $\frac{\Delta b}{b}$ числа b.

Предполагая опять все члены двойного неравенства (2) положительными, переписываем его в виде

$$\frac{1}{b+\Delta b} < \frac{1}{y} < \frac{1}{b-\Delta b}$$

и последовательно получаем:

$$\frac{1}{b+\Delta b} - \frac{1}{b} < \frac{1}{y} - \frac{1}{b} < \frac{1}{b-\Delta b} - \frac{1}{b},$$

$$-\frac{\Delta b}{b(b+\Delta b)} < \frac{1}{y} - \frac{1}{b} < \frac{\Delta b}{b(b-\Delta b)},$$

$$-\frac{\Delta b}{b+\Delta b} < \left(\frac{1}{y} - \frac{1}{b}\right) : \frac{1}{b} < \frac{\Delta b}{b-\Delta b}.$$

Дробь в левой части отличается от большей дроби $\frac{\Delta b}{b}$ на число второго порядка малости $\frac{(\Delta b)^2}{b(b+\Delta b)}$, а дробь в правой части — от меньшей дроби $\frac{\Delta b}{b}$ на число второго порядка малости $\frac{(\Delta b)^2}{b(b-\Delta b)}$. Вновь незначительно нарушая строгость рассуждения, приходим к неравенству

$$-\frac{\Delta b}{b} < \left(\frac{1}{y} - \frac{1}{b}\right) : \frac{1}{b} < \frac{\Delta b}{b}, \qquad (8)$$

говорящему, что граница относительной погрешности числа $\frac{1}{b}$ одинакова с границей относительной погрешности числа b. Рассматривая частное $\frac{a}{b}$ как произведение $a \cdot \frac{1}{b}$, приходим теперь к теореме:

Теорема III. *Граница относительной погрешности частного равна сумме границ относительных погрешностей делимого и делителя.*

Простым следствием теоремы II является формула

$$\frac{-n\Delta a}{a} < \frac{x^n - a^n}{a^n} < \frac{n\Delta a}{a},$$

выражающая следующее предложение:

Теорема IV. *Граница относительной погрешности степени с натуральным показателем равна произведению границы относительной погрешности основания на показатель степени.*

Полагая же $y = \sqrt[n]{x}$, имеем формулу $x = y^n$, $\frac{\Delta x}{x} = \frac{n\Delta y}{y}$, откуда

$$\frac{\Delta y}{y} = \frac{\Delta x}{x} : n,$$

что можно сформулировать в виде следующего предложения:

Теорема V. *Граница относительной погрешности корня с натуральным показателем равна частному от деления границы относительной погрешности подкоренного числа на показатель корня.*

Покажем применение этих теорем на следующем примере.

Пример 1. Вычислить значение

$$t=\sqrt{\frac{2hd}{g(d-d_1)}},$$

зная, что

$$h\approx 25{,}3\ (\pm 0{,}1), \qquad d\approx 19{,}32\ (\pm 0{,}01),$$
$$d_1\approx 0{,}998\ (\pm 0{,}0005), \qquad g\approx 982\ (\pm 0{,}5),$$

и указать границу абсолютной погрешности результата.

Решение. Здесь

$$\frac{\Delta t}{t}=\frac{0{,}5\,\Delta u}{u}, \quad u=\frac{2hd}{g(d-d_1)} \quad \text{(по теореме V)};$$

$$\frac{\Delta u}{u}=\frac{\Delta(2hd)}{2hd}+\frac{\Delta(gv)}{gv}, \quad v=d-d_1 \quad \text{(по теореме III)};$$

$$\frac{\Delta(2hd)}{2hd}=\frac{\Delta h}{h}+\frac{\Delta d}{d} \quad \text{(по теореме II; учтено, что } \Delta 2=0);$$

$$\frac{\Delta(gv)}{gv}=\frac{\Delta g}{g}+\frac{\Delta v}{v} \quad \text{(по теореме II)};$$

$$\Delta v=\Delta(d-d_1)=\Delta d+\Delta d_1 \quad \text{(по теореме I)}.$$

Окончательно

$$\frac{\Delta t}{t}=0{,}5\left[\frac{\Delta h}{h}+\frac{\Delta d}{d}+\frac{\Delta g}{g}+\frac{\Delta d+\Delta d_1}{d-d_1}\right].$$

Приближённое значение t находим с помощью таблицы четырёхзначных логарифмов, границы погрешности — посредством счётной линейки.

d	19,32
d_1	0,998
$v=d-d_1$	18,322
$\lg v$	1,2630
$\lg g$	2,9921
$\lg(gv)$	4,2551

$\lg 2$	0,3010
$\lg h$	1,4031
$\lg d$	1,2860
$\operatorname{clg}(gv)$	$\bar{5}$,7449
$\lg t^2$	$\bar{2}$,7350
$\lg t$	$\bar{1}$,3675
t	0,2331

$\Delta h=0{,}1$; $\Delta d=0{,}01$; $\Delta d_1=0{,}0005$; $\Delta g=0{,}5$;

$\Delta t:t=0{,}5\cdot[0{,}396+0{,}052+0{,}051+0{,}057]\ \%$
$=0{,}5\cdot 0{,}454\%$
$=0{,}227\%$

$\Delta t=0{,}227\%$ от $0{,}2331$
$=0{,}00053.$

Ответ. $t \approx 0{,}2331\ (\pm 0{,}00053) \approx 0{,}233\ (\pm 0{,}00053)$ или окончательно $t \approx 0{,}233\ (\pm 0{,}001)$.

Четвёртая значащая цифра результата, полученного с помощью четырёхзначных логарифмов, ненадёжна, а потому отброшена.

Для контроля и сравнения методов решим эту же задачу ещё раз, применяя способ границ и не пользуясь логарифмами.

	НГ	ВГ
h	25,2	25,4
$2h$	50,4	50,8
d	19,31	19,33
$2hd = a$	973,224	981,964
d_1	0,9975	0,9985
$d - d_1$	18,3115	18,3325
g	981,5	982,5
$g(d - d_1) = b$	17972	18012
$a : b = t^2$	0,05403	0,05465
t	0,2325	0,2338

$t \approx 0{,}2331\ (\pm 0{,}0007)$

$+\ \begin{array}{r} 0{,}2338 \\ 0{,}2325 \\ \hline 0{,}4663 : 2 = 0{,}23315 \end{array}$

$-\ \begin{array}{r} 0{,}2338 \\ 0{,}2325 \\ \hline 0{,}0013 : 2 = 0{,}00065 \end{array}$

Здесь учтены все источники ошибок, а результат получился практически тот же, что и по способу границ погрешностей.

Все формулы для вычисления границ погрешностей, полученные выше с помощью элементарных рассуждений, получаются много проще посредством дифференцирования.

Пусть $f(x, y)$ — некоторая дифференцируемая функция от двух переменных x и y; x_0 и y_0 — некоторые частные значения этих переменных. Полагая $x = x_0 + \alpha$, $y = y_0 + \beta$, $|\alpha| < \Delta x$, $|\beta| < \Delta y$ и считая числа Δx и Δy данными и настолько малыми по сравнению с x_0 и y_0, что их степенями и их произведениями можно пренебречь, ставим себе задачей найти наибольшее по абсолютной величине значение разности $f(x, y) - f(x_0, y_0)$ при условии, что приращения аргументов $\alpha = x - x_0$ и $\beta = y - y_0$ по абсолютной величине не превосходят соответственно Δx и Δy.

Как известно из курса математического анализа [1]), разность $f(x, y) - f(x_0, y_0)$ [«приращение» функции $f(x, y)$] состоит из двух частей: из *главной части*, которая называется *полным дифференциалом* функции и которую вычисляют по формуле

$$df = \frac{\partial f}{\partial x}\,dx + \frac{\partial f}{\partial y}\,dy$$

(x и y заменяются в производных через x_0 и y_0), и из членов высшего порядка малости. Здесь dx и dy — дифференциалы аргументов x и y или, что то же самое, приращения этих аргументов $x - x_0$, $y - y_0$, обозначенные у нас буквами α и β (символы Δx и Δy означают у нас высшие границы этих приращений). Если Δx и Δy — числа весьма малые, что мы и будем предполагать, то числа α и β — тоже весьма малые, и всеми членами высшего

[1]) Э. э. м., кн. 3, статья «Дифференциальное и интегральное исчисления».

порядка малости можно пренебрегать. Приходим к заключению, что

$$f(x_0+\alpha,\ y_0+\beta)-f(x_0,\ y_0)\approx\frac{\partial f}{\partial x}\alpha+\frac{\partial f}{\partial y}\beta.$$

Пользуясь известной теоремой о модуле суммы («модуль суммы не больше суммы модулей слагаемых») и замечая, что модуль произведения равен произведению модулей сомножителей, преобразуем полученное неравенство заменой $|\alpha|$ и $|\beta|$ через Δx и Δy; имеем:

$$|f(x_0+\alpha,\ y_0+\beta)-f(x_0,\ y_0)|\leqslant\left|\frac{\partial f}{\partial x}\right|\cdot|\alpha|+\left|\frac{\partial f}{\partial y}\right|\cdot|\beta|<$$
$$<\left|\frac{\partial f}{\partial x}\right|\cdot\Delta x+\left|\frac{\partial f}{\partial y}\right|\cdot\Delta y.$$

Численное значение последнего выражения (в нём x и y заменяются через x_0 и y_0) больше (по модулю) всех возможных при данных условиях значений разности между неизвестным точным значением функции $f(x_0+\alpha,\ y_0+\beta)$ и известным приближённым её значением $f(x_0,\ y_0)$, а потому может быть принято в качестве границы абсолютной погрешности числа $f(x_0,\ y_0)$ как приближения к $f(x,\ y)$.

Заключение это легко обобщается на функцию любого числа аргументов, и мы имеем формулу

$$\Delta f(x_0,\ y_0,\ z_0,\ \ldots)\approx\left|\frac{\partial f}{\partial x}\right|\cdot\Delta x+\left|\frac{\partial f}{\partial y}\right|\cdot\Delta y+\left|\frac{\partial f}{\partial z}\right|\cdot\Delta z+\ldots,\qquad(\text{A})$$

по которой и вычисляется граница абсолютной погрешности. Отдельные члены правой части указывают ту долю общей погрешности, какая обусловлена погрешностями значений каждой из переменных в отдельности. Полагая, что функция $f(x,\ y)$ последовательно равна $x+y$, $x-y$, xy, $\frac{x}{y}$, x^n, $\sqrt[n]{x}$, легко получаем с помощью формулы (A) все рассмотренные выше теоремы I — V. Так, взяв $f(x,\ y)=\frac{x}{y}$, имеем: $\frac{\partial f}{\partial x}=\frac{1}{y}$, $\frac{\partial f}{\partial y}=-\frac{x}{y^2}$, и формула (A) даёт (при положительных значениях x и y): $\Delta\left(\frac{x}{y}\right)=\frac{1}{y}\Delta x+$ $+\frac{x}{y^2}\Delta y$, или после почленного деления на $\frac{x}{y}$:

$$\Delta\left(\frac{x}{y}\right):\frac{x}{y}=\frac{\Delta x}{x}+\frac{\Delta y}{y},$$

т. е. теорему III.

Вот пример непосредственного применения формулы (A).

Пример 2. Вычислить сторону t треугольника, зная две другие его стороны $x\approx25{,}0\ (\pm0{,}2)$ *мм*, $y\approx30{,}0\ (\pm0{,}2)$ *мм* и угол между ними $z=60°{,}0\ (\pm0°{,}5)$.

Решение. Пользуясь формулой $t^2=x^2+y^2-2xy\cos z$ и применяя четырёхзначные таблицы, находим приближённое значение искомой стороны $t\approx27{,}84$ *мм*. Дифференцирование даёт:

$$\frac{\partial t}{\partial x}=\frac{x-y\cos z}{t},\quad\frac{\partial t}{\partial y}=\frac{y-x\cos z}{t},\quad\frac{\partial t}{\partial z}=\frac{xy\sin z}{t},$$

и для границы абсолютной погрешности найденного приближённого значения t получаем, применяя формулу (A):

$$\Delta t=0{,}359\cdot0{,}2+0{,}628\cdot0{,}2+23{,}3\cdot0{,}00873=0{,}072+0{,}126+0{,}203=0{,}401.$$

Здесь Δz выражено в радианах.

Итак, приходим к результату $t \approx 27{,}84\ (\pm 0{,}401)$ *мм* или после обычного округления $t \approx 27{,}8\ (\pm 0{,}46)$ *мм*; можно ручаться, что искомая сторона треугольника отличается от отрезка 27,8 *мм* меньше, чем на 0,46 *мм*. Тот же результат получается и при применении способа границ.

До сих пор мы имели дело с задачами, в которых по известным границам погрешностей данных требовалось найти границу погрешности результата. Но иногда приходится решать обратную задачу, а именно выяснять, с какой точностью необходимо знать данные, чтобы обеспечить некоторую наперёд указанную точность результата. При решении таких вопросов способ границ погрешностей имеет серьёзные преимущества перед способом границ. Не останавливаясь на такого рода задачах подробнее, ограничимся рассмотрением одного примера. Читателя, желающего ознакомиться с деталями, отсылаем к книгам [9] и [26].

С какой точностью надо взять вес p (в граммах) и объём v (в кубических сантиметрах) куска свинца, чтобы получить его плотность δ по формуле $\delta = \frac{p}{v}$ с погрешностью, не большей полупроцента?

На основании теоремы II пишем:

$$\frac{\Delta\delta}{\delta} = \frac{\Delta p}{p} + \frac{\Delta v}{v}.$$

Таким образом, сумма границ относительных погрешностей чисел p и v должна быть согласно заданию не больше $0{,}5\%$. Так как при взвешивании большая точность достигается гораздо легче, чем при измерении объёма, то отнесём на погрешность в определении веса только десятую часть этой погрешности, т. е. $0{,}05\%$, а остальные $0{,}45\%$ отнесём на погрешность в определении объёма. Если вес взятого куска свинца, определённый грубо приближённо, оказывается близким к 400 *г*, а его объём — близким к 40 $см^3$, то вес надо определить с погрешностью, не превосходящей $0{,}05\%$ от 400, т. е. 0,2 *г*, а объём — с погрешностью, не превосходящей 0,18 $см^3$. Имея в своём распоряжении весы, чувствующие 0,2 *г* при нагрузке в 400 *г*, и прибор для измерения объёма, позволяющий делать отсчёты до 0,1 $см^3$, мы достигнем требуемой точности в определении искомой плотности.

Мы ознакомились с двумя способами, дающими возможность делать вполне определённые заключения о точности результатов вычисления, зная точность данных, т. е. с двумя способами «строгого учёта погрешностей». Какой же из них, способ границ или способ границ погрешностей, заслуживает предпочтения?

Очевидными преимуществами способа границ являются: 1) чрезвычайная его простота, сводящая всю его теорию к одному основ-

ному принципу, применение которого на практике не вызывает никаких затруднений даже у мало подготовленного вычислителя; 2) его универсальность, так как применять его можно ко всяким числовым расчётам, от самых простых до самых сложных; 3) его строгость, позволяющая получать безусловно достоверные результаты благодаря возможности учитывать как погрешности от неточности данных, так и вычислительные погрешности; 4) контроль правильности вычислений, получающийся при сравнении результатов двух параллельных рядов операций.

Способ границ погрешностей превосходит способ границ в том отношении, что 1) позволяет заранее учитывать погрешность от неточности данных и даёт тем самым более или менее надёжное указание о той точности, с какой надо вести вычисление; 2) выясняет, какая доля общей погрешности результата обусловлена погрешностью каждого приближённого данного.

Способ границ погрешностей не отличается той безусловной строгостью, какая присуща способу границ как вследствие отбрасывания членов высшего порядка малости, так и в силу того, что учитываются только погрешности от неточности данных.

С первого взгляда кажется, что существенным недостатком способа границ является необходимость дважды повторять всё вычисление. Однако, сравнивая два решения одной и той же задачи, одно с учётом погрешностей по способу границ, другое — по способу границ погрешностей, убеждаемся, что общее количество выкладок в обоих случаях почти одинаково. Дело в том, что вычисление границы погрешности тоже требует некоторого труда. Правда, вычисление это можно упростить, пользуясь грубыми приближениями, но тогда либо получаются весьма ненадёжные результаты, либо излишне увеличиваются границы погрешностей. Необходимо отметить, что при вычислении по формуле, содержащей только действия второй и третьей ступеней, вычисление по способу границ погрешностей выполняется определённо скорее, чем по способу границ. Иначе обстоит дело, если в формулу наряду с действиями второй и третьей ступеней входят также действия первой ступени.

В случаях, когда требуется не абсолютная достоверность, а лишь более или менее высокая вероятность, как это обыкновенно бывает при обработке данных опыта и наблюдения, чаще пользуются вычислением границ погрешностей. В случаях же, когда такая абсолютная достоверность необходима (и по существу дела возможна), например при составлении математических таблиц, лучше употреблять способ границ.

В дидактическом отношении способ границ имеет очевидные преимущества перед способом границ погрешностей, и именно способ границ надо рекомендовать для первого ознакомления со способами строгого учёта погрешностей.

§ 10. Предельные погрешности результатов действий над приближёнными значениями. Правила подсчёта цифр

Если известно, сколько точных цифр имеет каждое приближённое данное, и если, кроме того, известны сами эти данные, то в каждом отдельном случае, основываясь на одном из рассмотренных выше способов (границ или границ погрешностей), мы можем установить, сколько заслуживающих доверия цифр содержит результат, и округлить его надлежащим образом. Естественно возникает вопрос: нельзя ли сделать какие-либо заключения о точности результатов, зная только число точных цифр каждого из данных, но не зная самих данных? Оказывается, такие заключения возможны и с успехом используются в вычислительной практике. Их часто называют «правилами подсчёта цифр» или «правилами округления результатов действий над приближёнными числами». Чтобы придти к этим правилам, надо установить, какого наибольшего значения достигают результаты действий над компонентами, имеющими данное число точных цифр. Назовём «предельной погрешностью» результата каждого действия границу его абсолютной погрешности, вычисленную в предположении, что компоненты даны с определённым числом точных цифр, и займёмся вычислением этих предельных погрешностей для разных случаев. Предельную погрешность будем обозначать буквой ε.

Проще всего определяется предельная погрешность алгебраической суммы. Если компоненты (слагаемые и вычитаемые) даны с каким угодно числом десятичных знаков, причём компонент с наименьшим числом десятичных знаков имеет k десятичных знаков (k — целое неотрицательное число), а всего имеется n компонентов, то $\varepsilon = 0{,}5 \cdot n \cdot 10^{-k}$. Истинная абсолютная погрешность суммы равняется этой предельной погрешности в случае, когда все компоненты имеют по k десятичных знаков и каждый имеет максимальную возможную погрешность в пол-единицы разряда последней цифры, причём все — одного знака. Таким образом, эта предельная погрешность для общего случая не может быть понижена.

Эти соображения являются достаточным обоснованием следующего практического правила:

Правило I подсчёта цифр. *При сложении и вычитании приближённых чисел в результате следует сохранять столько десятичных знаков, сколько их в приближённом данном с наименьшим числом десятичных знаков.*

Напоминаем, что десятичными знаками числа называются те его цифры, какие расположены справа от знака дробности. Все приближённые данные предполагаются округлёнными так, чтобы в них оставались только цифры, заслуживающие доверия. Целые числа с нулями справа, заменяющими неизвестные цифры, рекомендуется писать в виде произведений на некоторую степень 10 с целым показателем (например, приближённое число 347 000, являющееся результа-

том округления некоторого точного числа до разряда тысяч, лучше писать в виде $347 \cdot 10^3$ или $3{,}47 \cdot 10^5$ и т. д.).

Необходимость округления, указываемого настоящим правилом, становится очевидной, если рассмотреть какой-либо конкретный пример, заменяя особыми знаками, например знаками вопроса, неизвестные цифры приближённых данных. Пусть, например, требуется найти сумму трёх указанных ниже приближённых слагаемых, из которых первое является результатом округления неизвестного истинного значения до трёх десятичных знаков, второе — до 1, третье — до 2. Производя сложение обычным порядком так, как это делается в случае точных компонентов, мы получаем число 87,943, в котором цифры сотых и тысячных никакого доверия не заслуживают и должны быть отброшены, что и рекомендует сделать правило I.

$$\begin{array}{r} 0{,}423?.. \\ +\,72{,}8???.. \\ 14{,}72??.. \\ \hline 87{,}943?.. \\ \hline 87{,}9 \end{array}$$

В настоящем примере истинная абсолютная погрешность суммы может лишь незначительно превзойти пол-единицы разряда последней цифры, но легко указать случаи, когда она будет составлять несколько единиц этого разряда. Заслуживает ли доверия эта последняя цифра? Этот вопрос будет рассмотрен в §§ 11 и 12.

Переходя к умножению, формулируем следующую теорему о предельной погрешности:

Теорема 1. *Произведение двух приближённых чисел, имеющих каждое k точных значащих цифр, имеет предельную погрешность, равную* 5,5 *единицы разряда k-й значащей цифры; это значение предельной погрешности снижается до* 5,05 *для случая, когда один из приближённых сомножителей имеет k точных значащих цифр, другой $k+1$ цифру, и до* 5, *когда один из сомножителей имеет k точных значащих цифр, другой же точен.*

Вот пример случая, когда истинная абсолютная погрешность произведения близка к указанной в теореме предельной погрешности: $x = 100{,}499$, $y = 9{,}99499$, $xy = 1004{,}486\ldots$, $a = 100$, $b = 9{,}99$, $ab = 999$. Здесь произведение приближённых трёхзначных чисел a и b отличается от произведения точных чисел x и y на 5,486... единиц разряда 3-й значащей цифры.

Приводим доказательство теоремы, ограничиваясь случаем $k = 3$ (легко видеть, что для произвольного значения k это доказательство сохраняет силу, требуя лишь несколько более длинной записи). Положение знака дробности в данных безразлично; будем для определённости считать запятую поставленной в первом из данных после третьей значащей цифры, во втором — после первой. Пусть точные значения сомножителей a и b суть x и y, так что $x = a + \alpha$, $y = b + \beta$, где α и β — истинные абсолютные погрешности при-

ближённых чисел a и b. Согласно сказанному выше имеем:

$$100 \leqslant a \leqslant 999; \quad 1{,}00 \leqslant b \leqslant 9{,}99; \quad |\alpha| \leqslant 0{,}5; \quad |\beta| < 0{,}005.$$

Надо дать оценку разности $xy - ab = a\beta + b\alpha + \alpha\beta$ в единицах разряда третьей значащей цифры произведения ab. Имеем:

$$|xy - ab| \leqslant 0{,}005\,a + 0{,}5\,b + 0{,}0025$$

или

$$|xy - ab| \leqslant 0{,}005\,(a + 100\,b) + 0{,}0025.$$

Рассмотрим порознь случаи, когда произведение ab имеет 1) три и 2) четыре цифры до знака дробности. Неравенство $100 \cdot 1{,}00 \leqslant ab \leqslant 999 \cdot 9{,}99$ показывает, что только эти два случая и возможны.

В первом случае $ab \leqslant 999{,}99$; $100\,b \leqslant \frac{p^2}{a}$, где $p^2 = 99\,999$, а потому

$$a + 100\,b \leqslant a + \frac{p^2}{a}.$$

Дифференцируя функцию $a + \frac{p^2}{a}$ по a, убеждаемся, что при непрерывном изменении a от $a = 100$ до $a = 999$ она сначала убывает (от значения 1099,99 при $a = 100$ до значения $2p = 632{,}4\ldots$ при $a = p = 316{,}2\ldots$), потом растёт $\left(\text{от значения } 2p \text{ при } a = p \text{ до значения } 1099 + \frac{99}{999} \text{ при } a = 999\right)$. Но, принимая во внимание, что сумма $a + 100\,b$ принимает при сделанных предположениях только целые значения, заключаем, что наибольшее возможное её значение есть 1099, а потому

$$|xy - ab| \leqslant 0{,}005 \cdot 1099 + 0{,}0025 = 5{,}4975 < 5{,}5,$$

что и доказывает первую часть теоремы для случая, когда произведение имеет три значащие цифры до знака дробности.

Во втором случае, когда произведение ab имеет не три, а четыре цифры до знака дробности, наибольшее возможное значение его погрешности вычисляется гораздо проще. Действительно, теперь

$$|xy - ab| \leqslant 0{,}005 \cdot 999 + 0{,}5 \cdot 9{,}99 + 0{,}0025 = 9{,}9925 < 10.$$

При четырёх значащих цифрах до знака дробности третья значащая цифра есть цифра десятков, и у нас, следовательно, доказано, что число $|xy - ab|$ меньше одной единицы разряда третьей значащей цифры произведения. Первая часть теоремы тем самым доказана и для второго случая.

Если один из приближённых сомножителей имеет $k = 3$ точных значащих цифры, другой $k + 1 = 4$, то, рассуждая по предыдущему, имеем:

$$100 \leqslant a \leqslant 999; \quad 1{,}000 \leqslant b \leqslant 9{,}999; \quad |\alpha| \leqslant 0{,}5; \quad |\beta| \leqslant 0{,}0005;$$

$$|xy - ab| \leqslant 0{,}0005\,a + 0{,}5\,b + 0{,}00025 = 0{,}0005\,(a + 1000\,b) + 0{,}00025.$$

Если произведение ab имеет три цифры левее запятой, то

$$ab \leqslant 999{,}999; \quad 1000\,b \leqslant \frac{p^2}{a},$$

где $p^2 = 999\,999$, а потому

$$a + 1000\,b \leqslant a + \frac{p^2}{a}.$$

Эта последняя сумма при изменении a от 100 до 999 только убывает, так как её минимум достигается при $a = p = 999{,}99\ldots$, и следовательно, наи-

большее возможное её значение есть $100 + 9999{,}99 = 10\,099{,}9\ldots$; сумма же $a + 1000\,b$, принимающая только целые значения, не может превзойти числа 10 099. Отсюда заключаем, что

$$|xy - ab| \leqslant 0{,}0005 \cdot 10\,099 + 0{,}00025 = 5{,}04975 < 5{,}05.$$

Если же произведение ab имеет до запятой четыре цифры, то

$$|xy - ab| \leqslant 0{,}4995 + 4{,}9995 + 0{,}00025 = 5{,}49925 < 5{,}5$$

или 0,55 единицы разряда третьей значащей цифры. Тем самым доказана и вторая часть теоремы.

Переходя к третьей её части, имеем:

$$x = a + \alpha;\quad 100 \leqslant a \leqslant 999;\quad |\alpha| \leqslant 0{,}5;\quad y = b;\quad 1 \leqslant b < 10;$$
$$|xy - ab| \leqslant 0{,}5\,b \leqslant 5.$$

Когда произведение содержит три значащие цифры левее знака дробности, его погрешность не больше пяти единиц разряда третьей значащей цифры, а когда четыре, т. е. когда третья значащая цифра есть цифра десятков, то не больше 0,5 единицы разряда третьей значащей цифры.

Теорема доказана полностью.

Основываясь на формулированной выше теореме, делаем практически важные заключения. Если один из сомножителей — приближённое число с k точными значащими цифрами, а другой сомножитель не менее точен, т. е. является либо приближённым числом, имеющим тоже k или больше точных значащих цифр, либо точным, то в произведении нет смысла сохранять больше чем k значащих цифр: уже k-я значащая цифра сомнительна. Возникает даже вопрос о том, стоит ли сохранять эту k-ю значащую цифру (этот вопрос будет решён положительно в §§ 11 и 12). Далее, имея два сомножителя с разным числом значащих цифр, без ущерба для точности результата можно предварительно округлить более точный сомножитель так, чтобы в нём было только одной значащей цифрой больше, чем в менее точном, имеющем k точных значащих цифр: предельная погрешность в результате такого округления едва меняется, а именно, растёт самое большее с 5 до 5,05 единицы разряда k-й значащей цифры произведения. Но эту лишнюю («запасную») цифру в более точном сомножителе сохранять стоит, так как её отбрасывание вызывает заметное увеличение предельной погрешности произведения, а именно, с 5,05 до 5,5 единицы k-й значащей цифры.

Исследуя аналогичным образом частное, приходим к следующему предложению:

Теорема 2. *Частное от деления двух приближённых чисел, данных каждое с k точными значащими цифрами, имеет предельную погрешность, равную* 10 *единицам k-й значащей цифры; это значение предельной погрешности снижается до* 5,5 *единицы, когда один из компонентов имеет k точных значащих цифр, другой $k+1$ цифру; до* 5,22 *единицы, когда делимое — число точное, а делитель имеет k точных значащих цифр, и до* 5 *еди-*

ниц, когда делимое имеет k точных значащих цифр, а делитель — число точное.

Доказательство этой теоремы, проводимое аналогично доказательству предыдущей теоремы, опускаем. Оценка предельной погрешности произведения и частного делает очевидной целесообразность следующего практического правила.

Правило II подсчёта цифр. *При умножении и делении следует сохранять в результате столько значащих цифр, сколько их имеет приближённое данное с наименьшим числом значащих цифр.*

Сомнение относительно целесообразности сохранения k-й значащей цифры произведения, ошибка в которой может доходить до 5,5 единицы, и тем более k-й значащей цифры частного, ошибка в которой может доходить до 10 единиц, будет устранено соображениями, изложенными в §§ 11 и 12.

Целесообразность этого правила, как и правила I, хорошо уясняется путём рассмотрения конкретных примеров с заменой неизвестных цифр знаками вопроса. Приводим четыре таких примера, понятных без особых пояснений. Заслуживающие доверия цифры отделены вертикальной пунктирной чертой. Подробнее о такого рода примерах можно прочесть в книге [2а].

	9,56?		3,143?	936	?:218? = 4,29	65	4,7?:2,6? = 250
×	2,18?		0,85?	872	?	52	? (лучше $2{,}5 \cdot 10^2$).
	?????		??????	64	??	13	47
7	648?	1	5715?	43	6?	13	0?
9	56?	25	144?	20	4??		47
191	2?	26	7155??	19	62?		
208	408??	2,7			78?		
20,8							

Переходя к действиям III ступени (возведению в степень и извлечению корня) и ограничиваясь только случаями, когда показателями степени и корня являются числа 2 и 3, без труда доказываем следующие две теоремы.

Теорема 3. *Квадрат и куб приближённого числа, имеющего k точных значащих цифр, может иметь абсолютную погрешность, приближающуюся соответственно к* 3,5 *единицы и* 7,2 *единицы k-й значащей цифры, но никогда не превосходящую этих предельных значений.*

Теорема 4. *Квадратный и кубический корень из приближённого числа, имеющего k точных значащих цифр, может иметь абсолютную погрешность, приближающуюся соответственно к* 0,81 *и* 0,79 *единицы разряда k-й значащей цифры, но никогда не превосходящую этих предельных значений.*

Эти теоремы дают основание установить для возведения в квадрат и куб и для извлечения квадратного и кубического корня такие два правила:

Правило III подсчёта цифр. *При возведении в квадрат и куб в результате следует сохранять столько значащих цифр, сколько их имеет возводимое в степень приближённое число.*

Правило IV подсчёта цифр. *При извлечении квадратного и кубического корней в результате следует брать столько значащих цифр, сколько их имеет приближённое значение подкоренного числа.*

Приведённые выше значения предельных погрешностей, а также соображения, изложенные ниже в §§ 11 и 12, позволяют сделать следующие примечания к этим двум правилам: последняя цифра квадрата и особенно куба при этом менее надёжна, чем последняя цифра основания, а последняя цифра квадратного и особенно кубического корня более надёжна, чем последняя цифра подкоренного числа.

Откладывая рассмотрение практических применений правил подсчёта цифр до § 13, отметим сейчас только то обстоятельство, что указанные выше значения предельных погрешностей при применении правил подсчёта цифр увеличиваются ещё максимум на 0,5 в каждом случае за счёт погрешности, вносимой округлением результата. В табличке на стр. 411 приведены как указанные выше, так и эти увеличенные значения предельных погрешностей.

Небезынтересно подметить связь, существующую между правилами подсчёта цифр (I—IV) и теоремами о границах абсолютных и относительных погрешностей, установленными в § 9. При сложении и вычитании приближённых чисел приходится складывать границы абсолютных погрешностей данных, определяемые числом точных десятичных знаков в этих данных, а при умножении и делении складываются границы относительных погрешностей данных, определяемых числом точных значащих цифр в данных. Это обстоятельство объясняет, почему при сложении и вычитании приходится подсчитывать десятичные знаки, а при умножении и делении — значащие цифры. Умножение границы относительной погрешности на показатель степени при возведении в степень и её деление на показатель корня при извлечении корня делают понятными снижение точности в первом случае и её повышение во втором.

§ 11. Средние квадратические погрешности результатов действий над приближёнными числами. Принцип академика А. Н. Крылова

В тех случаях, когда мы имеем возможность, кроме границы погрешности, т. е. наибольшего возможного её значения, установить также и истинную погрешность результата, мы каждый раз видим, что эта истинная погрешность значительно меньше наибольшей возможной. Явление это бывает выражено тем ярче, чем больше приближённых чисел участвует в вычислении. Возьмём, например, сумму четырёхзначных логарифмов 20 последовательных чисел от 11 до 30 включительно. Граница абсолютной погрешности каждого

такого логарифма есть 0,00005, а суммы 20 логарифмов есть $0{,}00005 \times 20 = 0{,}001$. Произведя сложение логарифмов, получим сумму 25,8638, причём ручаться можем только за то, что истинное значение этой суммы больше чем 25,8628 и меньше чем 25,8648. Если же взять восьмизначные логарифмы тех же 20 чисел и опять произвести сложение, то получим сумму 25,86389705. Как видим, истинная погрешность первой суммы не достигает даже одной десятитысячной и составляет, таким образом, примерно десятую часть своей теоретической границы.

Такое расхождение между истинной и наибольшей возможной погрешностями объясняется, прежде всего, тем, что при разыскании этой наибольшей возможной погрешности мы всегда предполагаем самое неблагоприятное стечение обстоятельств. Так, в только что разобранном примере мы считаем границей погрешности каждого слагаемого пол-единицы разряда последней его цифры. Между тем истинные погрешности этих слагаемых могут принимать, и на самом деле принимают, всевозможные значения от $-0{,}5$ до $+0{,}5$ единицы этого разряда. Далее, положительные погрешности, встречаясь примерно одинаково часто с отрицательными, в более или менее значительной степени их уравновешивают, процесс накопления погрешностей идёт параллельно процессу взаимной их компенсации, и в результате вероятность того, что погрешность суммы примет большое, т. е. близкое к границе, значение, становится крайне малой. Конечно, подбирая слагаемые искусственно, можно получить погрешность суммы, как угодно близкую к границе. При отсутствии же такого искусственного подбора это становится весьма мало вероятным. Методами теории вероятностей можно установить, как часто должно встречаться то или иное значение погрешности суммы.

Результаты теоретического исследования подтверждаются и прямым опытом. Так, например, был проделан такой опыт. Было взято 440 сумм по 20 логарифмов каждая, сначала с 5, потом с 7 десятичными знаками, и определены разности этих сумм, т. е. приближённые значения погрешностей сумм пятизначных логарифмов. Нижеприведённые числа показывают довольно близкое согласие результатов опыта и тех чисел, какие даются теорией.

Погрешность суммы лежит между	По теории	Число случаев в действительности
0 и 100	56,14%	65%
100 и 200	31,72%	28%
200 и 300	10,13%	6%
300 и 400	1,82%	1%
400 и 500	0,18%	0%
500 и 1000	0,01%	0%

Погрешности здесь выражены в десятимиллионных долях (в единицах разряда последней цифры семизначных логарифмов). Граница

абсолютной погрешности суммы 20 слагаемых, имеющих каждое пять точных десятичных знаков, равна $0{,}5 \cdot 10^{-5} \cdot 20$ или 1000 десятимиллионных, но эта граница далеко не достигнута во всех 440 случаях.

В практических вычислениях нельзя не считаться с этой малой вероятностью больших, т. е. близких к предельным, погрешностей.

Строгий учёт погрешностей результатов вычислений, требующий, как мы видели в §§ 8 и 9, немалой дополнительной работы, применяется на практике очень редко. Обыкновенно вычислители довольствуются тем, что ведут вычисление с определённым числом цифр (значащих цифр или десятичных знаков), сохраняя в результатах одну, иногда две сомнительные цифры (см. например, конец статьи [6]).

Иногда выставляют требование, чтобы употребляемые на практике приближённые числа имели погрешности, не превосходящие единицы разряда последней сохраняемой цифры. Вот, например, что говорит об этом акад. А. Н. Крылов в своей книге [10]:

«Результат всякого вычисления и измерения выражается числом; условимся писать эти числа так, чтобы по самому их начертанию можно было судить о степени точности; для этого стоит только принять за правило писать число так, чтобы в нём все значащие цифры, кроме последней, были верны, и лишь последняя цифра была бы сомнительна и притом не более как на одну единицу».

Если понимать это требование буквально, то оно весьма трудно исполнимо. Действительно, чтобы его соблюсти, необходим, во-первых, постоянный строгий учёт погрешностей, и, во-вторых, на каждом почти шагу приходилось бы сильно округлять результаты. Например, четырёхзначные логарифмы, полученные в результате сложения трёх четырёхзначных же логарифмов, имеют границу погрешности в $1\frac{1}{2}$ единицы разряда последней цифры, а потому, придерживаясь этого правила, их пришлось бы округлить до трёх десятичных знаков. Однако стоит только добавить в вышеприведённом правиле одно лишь слово «в среднем», и мы получаем основной важности принцип, который позволяет рационально обосновать целый ряд практических правил вычисления с приближёнными числами. Этот «основной принцип обыкновенных вычислений», т. е. вычислений без строгого учёта погрешностей, формулируем в окончательном виде так:

Принцип А. Н. Крылова. *Приближённое число надо писать так, чтобы в нём все значащие цифры, кроме последней, были верны и лишь последняя цифра была бы сомнительна и притом «в среднем» не более как на одну единицу.*

Это добавление «в среднем» мы будем понимать в том смысле, что здесь речь идёт не о границе погрешности, а о средней

квадратической погрешности, т. е. о корне квадратном из среднего значения квадрата погрешности.

Чтобы яснее её себе представить, решим такую задачу:

Найти среднюю квадратическую погрешность округления, состоящего в отбрасывании одной только цифры, считая все возможные значения этой цифры равновероятными, т. е. встречающимися (при большом числе округлений) одинаково часто. Следовательно, равновероятны следующие значения погрешности округления (в единицах разряда последней цифры): — 0,5; — 0,4; — 0,3; — 0,2; — 0,1; 0,0; 0,1; 0,2; 0,3; 0,4; 0,5.

Всего здесь 11 значений погрешностей. Возьмём их квадраты, найдём сумму этих квадратов, разделим сумму на 11 и извлечём из частного квадратный корень. Это и даст искомую среднюю квадратическую погрешность округления, равную

$$\sqrt{\frac{2}{11}(0{,}25+0{,}16+0{,}09+0{,}04+0{,}01)}=$$

$$=\sqrt{\frac{2\cdot 0{,}55}{11}}=\sqrt{0{,}1}\approx 0{,}316.$$

Если округление состоит в отбрасывании не одной, а двух цифр, то будем иметь уже не 11, а 101 значение погрешности (от — 0,50 до + 0,50), и средняя квадратическая погрешность округления оказывается равной 0,292. При её вычислении, во избежание сложения длинного ряда чисел, можно воспользоваться формулой

$$1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

Если, наконец, округление состоит в отбрасывании бесконечной последовательности цифр, то, как показывает расчёт, основанный на переходе к пределу или на применении интегрального исчисления, средняя квадратическая погрешность округления оказывается равной числу $\sqrt{3}:6=0{,}289$.

Чтобы использовать принцип А. Н. Крылова в приведённой выше второй его формулировке для вывода правил действий над приближёнными числами, надо найти средние квадратические погрешности результатов отдельных действий. Покажем, как вычисляется средняя квадратическая погрешность суммы n приближённых слагаемых, каждое из которых является результатом округления некоторого точного числа до k-го десятичного знака.

Пусть дано приближённое значение a, имеющее k точных десятичных знаков; будем его рассматривать как результат округления числа x_i, имеющего $m>k$ десятичных знаков, причём возможны всего $10^{m-k}+1=p$ различных значений x_i, которые можно считать равновероятными. Если, например, $a=74{,}62$; $k=2$; $m=5$, то

$p = 1001$; $x_1 = 74{,}61500$; $x_2 = 74{,}61501$; $x_3 = 74{,}61502$; ...; $x_{1000} = 74{,}62499$; $x_{1001} = 74{,}62500$. Истинная абсолютная погрешность этого значения a, равная $x_i - a$, имеет, таким образом, всего p равновероятных значений от $x_1 - a = -0{,}500 \cdot 10^{-k}$ до $x_p - a = +0{,}500 \cdot 10^{-k}$, причём

$$\sum_{i=1}^{p} (x_i - a) = 0, \qquad \frac{\sum_{i=1}^{p} (x_i - a)^2}{p} = \sigma_a^2.$$

Символ σ_a означает здесь среднюю квадратическую погрешность числа a, причём при $k = 2$, $m = 5$, как легко видеть,

$$\sigma_a = \sqrt{\frac{2 \cdot \frac{1}{6} \cdot 500 \cdot 501 \cdot 1001 + 1}{1001}} \cdot 10^{-5} \approx 0{,}289 \cdot 10^{-3}.$$

При $m \to \infty$

$$\sigma_a \to \frac{1}{6}\sqrt{3} \cdot 10^{-k}.$$

Одновременно рассматриваем второе приближённое число b, совершенно независимое от первого, тоже имеющее k точных десятичных знаков и тоже являющееся результатом округления точного числа y_j, имеющего $m > k$ десятичных знаков; возможны всего $10^{m-k} + 1 = p$ значений y_j, которые опять-таки считаем равновероятными. Как и в первом случае,

$$\sum_{j=1}^{p} (y_j - b) = 0, \qquad \frac{\sum_{j=1}^{p} (y_j - b)^2}{p} = \sigma_b^2,$$

причём $\sigma_b = \sigma_a$.

Берём сумму $c = a + b$, представляющую собой приближённое значение точной суммы $z_{ij} = x_i + y_j$, способной принимать любое из p^2 возможных и равновероятных значений (любое из p возможных значений x_i комбинируется с любым из p возможных значений y_j). Имея

$$(z_{ij} - c)^2 = [(x_i - a) + (y_j - b)]^2 = \\ = (x_i - a)^2 + (y_j - b)^2 + 2(x_i - a)(y_j - b),$$

сначала фиксируем j и берём p таких равенств для значений i от 1 до p. Получив равенство

$$\sum_{i=1}^{p} (z_{ij} - c)^2 = \sum_{i=1}^{p} (x_i - a)^2 + p(y_j - b)^2 + 2(y_j - b) \sum_{i=1}^{b} (x_i - a),$$

в котором третье слагаемое равно нулю, суммируем все такие равен-

ства по значку j, принимающему p значений (от 1 до p), и получаем:

$$\sum_{j=1}^{p}\sum_{i=1}^{p}(z_{ij}-c)^2=p\sum_{i=1}^{p}(x_i-a)^2+p\sum_{j=1}^{p}(y_j-b)^2.$$

После почленного деления на p^2 приходим к равенству

$$\sigma_c^2=\sigma_a^2+\sigma_b^2,$$

говорящему, что при сделанных предположениях *квадрат средней квадратической погрешности суммы равен сумме квадратов средних квадратических погрешностей слагаемых.*

Это заключение сразу обобщается на любое число слагаемых (как легко видеть, оно сохраняет силу и при более общих предположениях, чем сделано выше). Рассматривая сумму n слагаемых, удовлетворяющих указанным выше требованиям, имеем:

$$\sigma_s^2=\sigma_a^2+\sigma_b^2+\ldots+\sigma_n^2,\quad \sigma_a=\sigma_b=\ldots=\sigma_n,\quad \sigma_s^2=n\sigma_a^2,$$

$$\sigma_s=\sigma_a\sqrt{n}.$$

Итак, *средняя квадратическая погрешность суммы равноточных слагаемых пропорциональна корню квадратному из их числа.* Отсюда следует, что средняя квадратическая погрешность суммы n приближённых слагаемых, каждое из которых есть результат округления некоторого точного числа до k-го десятичного знака, равна $\frac{1}{6}\cdot\sqrt{3}\cdot\sqrt{n}\cdot 10^{-k}$ или приближённо $0{,}289\sqrt{n}\cdot 10^{-k}$.

Возвращаясь к принципу акад. А. Н. Крылова, пишем неравенство $\frac{1}{6}\sqrt{3}\cdot\sqrt{n}\leqslant 1$, которое даёт: $n\leqslant 12$.

Итак, имея не более 12 приближённых слагаемых, полученных посредством округления до одного и того же десятичного знака, можно сохранять все десятичные знаки суммы. На практике часто превосходят это число 12. Описанный выше опыт со сложением логарифмов показывает, что и при $n=20$ стоит сохранять все знаки суммы.

Любопытно сопоставить соответствующие значения предельной погрешности ε и средней квадратической погрешности суммы для разных n. Приводим табличку для n от 2 до 12, выражая ε и σ в единицах разряда k-го десятичного знака.

n	2	3	4	5	6	7	8	9	10	11	12
ε	1	1,5	2	2,5	3	3,5	4	4,5	5	5,5	6
σ	0,409	0,501	0,578	0,647	0,708	0,765	0,818	0,867	0,915	0,960	1,000

Изложенный вывод значения σ для суммы n слагаемых существенно упрощается, если использовать простейшие теоремы о ве-

роятностях и применить интегральное исчисление. Не вызывает тогда затруднений и вычисление средних квадратических погрешностей результатов других действий. Ограничимся приведением таблицы, в которой сопоставлены значения предельных погрешностей и средних квадратических погрешностей.

Результат действия	ε	σ	ε_1
Алгебраическая сумма n слагаемых	$0{,}5n$	$0{,}289\sqrt[4]{n}$	$0{,}5n$
Произведение двух k-значных приближённых чисел	5,5	0,626	6
Произведение k-значного приближённого числа на точное	5	0,442	5,5
Произведение k-значного приближённого на $(k+1)$-значное приближённое	5,05	0,445	5,55
Частное от деления k-значного приближённого на k-значное приближённое	10	0,576	10,5
Частное от деления k-значного приближённого на точное	5	0,151	5,5
Частное от деления k-значного приближённого на $(k+1)$-значное приближённое	5,5	0,391	6
Частное от деления точного на k-значное приближённое	5,22	0,425	5,72
Частное от деления $(k+1)$-значного приближённого на k-значное приближённое	5,5	0,427	6
Квадрат k-значного приближённого числа	3,5	0,705	4
Куб k-значного приближённого числа	7,13	1,059	7,63
Квадратный корень из k-значного приближённого числа	0,81	0,221	1,31
Кубический корень из k-значного приближённого числа	0,79	0,185	1,29

Все числа, приведённые в столбцах ε, σ, ε_1, выражены в единицах разряда k-й значащей цифры, кроме чисел первой строки, выраженных в единицах разряда k-го десятичного знака.

Сопоставление значений предельной погрешности (ε) и средней квадратической погрешности (σ) подтверждает целесообразность указанных в § 10 правил подсчёта цифр, показывая, что они удовлетворяют принципу акад. А. Н. Крылова. Числа столбца ε_1 получены путём прибавления 0,5 к соответствующим числам столбца ε и показывают, какого значения может достигнуть погрешность после отбрасывания всех цифр, следующих за k-й значащей.

§ 12. Распределение погрешностей в результатах вычислений

Сопоставление предельных и средних квадратических погрешностей, выполненное в таблице § 11, с полной определённостью говорит о малой вероятности больших погрешностей (т. е. погрешностей, близких к предельным): если, например, в произведении двух k-значных приближённых чисел предельная погреш-

ность 5,5, а средняя квадратическая только 0,626 (единицы разряда k-й значащей цифры), то в подавляющем большинстве случаев фактическая погрешность должна быть очень небольшой и лишь в редких случаях приближаться к предельной. Естественно, возникает желание установить более точно картину распределения погрешностей, т. е. выяснить, как часто встречаются погрешности, заключённые в определённых интервалах.

Решение этой задачи требует несколько углублённых сведений по теории вероятностей, и мы ограничимся ссылками на книгу акад. Крылова [10], где эта задача решена для суммы (стр. 195—204). Применяя формулы, приведённые у акад. Крылова, к сумме 20 слагаемых, полученных округлением до одного и того же десятичного знака произвольных точных чисел, получаем результаты, указанные выше (на стр. 406): погрешность, не превосходящая одной единицы разряда этого десятичного знака, получается в 56,14% всех случаев, погрешность от одной до двух единиц — в 31,72% всех случаев, от двух до трёх единиц — в 10,13%, от трёх до четырёх единиц — в 1,82%, от четырёх до пяти единиц — в 0,18%, а от пяти до 10 единиц — только в 0,01% всех случаев, т. е. в среднем один раз на 10 000 случаев сложения; погрешность, превосходящая 10, здесь невозможна. Рассматривая произведение двух k-значных приближённых чисел, полученных посредством округления до k-й значащей цифры произвольных точных чисел: имеем результат с погрешностью, не превосходящей одной единицы разряда k-й значащей цифры, в 91,51% всех случаев, с погрешностью от одной до двух единиц — в 5,87%, от двух до трёх единиц — в 2,09%, от трёх до четырёх единиц — в 0,47%, от четырёх до пяти с половиной единиц — в 0,06% всех случаев; погрешность в 5,5% — предельная.

Нетрудно поставить опыт, подтверждающий правильность расчёта. Согласие между опытом и теорией тем больше, чем больше рассмотрено случаев умножения. При коллективной работе группы в 20—30 человек проведение такого опыта займёт всего 15—20 минут. Пусть каждый участник возьмёт несколько пар совершенно произвольных трёхзначных чисел и перемножит числа каждой пары, а затем округлит взятые числа до двух значащих цифр и вновь перемножит эти уже округлённые числа каждой пары. Поставив знаки дробности во взятых числах так, чтобы произведения содержали по две цифры левее запятой, находим разности произведений неокруглённых и округлённых чисел каждой пары. Например, берём числа 492 и 927, произведение которых 456 084, и после их округления до двух значащих цифр получаем числа 49 и 93, произведение которых 4557. Поставив в каждом сомножителе запятую после первой цифры, имеем: $4{,}92 \cdot 9{,}27 = 45{,}6084$ и $4{,}9 \cdot 9{,}3 = 45{,}57$. Здесь разница между произведениями точных и приближённых сомножителей составляет 0,0384 (единицы разряда второй значащей цифры).

Когда все эти операции выполнены, останется подсчитать число случаев, в которых разница заключается в границах от 0 до 1, от 1 до 2, от 2 до 3, от 3 до 4, от 4 до 5, от 5 до 5,5 и установить, сколько процентов от общего числа всех взятых пар составляют соответствующие числа.

Вот результаты одного подобного опыта, проведённого над 200 парами взятых наудачу пятизначных чисел, округляемых в ходе опыта до трёх значащих цифр каждая. Погрешности произведений округлённых чисел заключались между 0 и 1 (разряда третьей значащей цифры) в 186 случаях, т. е. в 93% всего числа испытаний (по теории должно быть 91,51%), между 1 и 2 — в 10 случаях, т. е. в 5% всего числа испытаний (по теории 5,87%), между 2 и 3 — в трёх случаях, т. е. в 1,5% всего числа испытаний (по теории 2,09%), между 3 и 4 — в одном только случае, т. е. в 0,5% всего числа испытаний (по теории 0,47%). Погрешность, превосходящая 4, не встретилась ни разу (теория для интервала от 4 до 5,5 даёт 0,06%).

Таким образом, теоретические исследования распределения погрешностей в сумме и произведении удовлетворительно согласуются с опытом. Подобное же положение имеет место и с частными, квадратами, кубами, квадратными и кубическими корнями. Правила подсчёта цифр I, II, III получают новое подтверждение. Следуя им, нельзя гарантировать точности последней цифры результата, но в большинстве случаев погрешность в этой цифре столь незначительна, что было бы неразумно вовсе её отбрасывать; вместе с тем неразумно было бы сохранять больше цифр, чем рекомендуют правила.

Само собой разумеется, что в случаях особо ответственных вычислений, когда нужна абсолютная надёжность результата, правила подсчёта цифр неприменимы: здесь необходим строгий учёт погрешностей по способу границ или по способу границ погрешностей. Но в обычных вычислениях, когда строгий учёт погрешностей не проводится, правила подсчёта цифр дают надёжные указания о рациональном округлении всех получаемых результатов.

§ 13. Практические применения правил подсчёта цифр. Сводка этих правил

Правила I—IV, рассмотренные в § 10, говорят о том, как надо округлять результаты отдельных действий над приближёнными числами. Такое округление иногда понижает имеющуюся в неокруглённом результате погрешность, иногда повышает её.

Пусть, например, даны числа $x = 33{,}1$ и $y = 2{,}52$ и найдено их произведение $xy = 83{,}412$. Округляя их до двух значащих цифр имеем: $a = 33$ и $b = 2{,}5$; произведение этих приближённых дву

значных чисел равно 82,5 и отличается от точного своего значения на разность $83{,}412 - 82{,}5 = 0{,}912$. Но после округления приближённого произведения согласно правилу II до двух значащих цифр, а именно, после замены его числом 82, эта разница увеличивается до $83{,}412 - 82 = 1{,}412$. Таким образом, в данном случае фактическая погрешность результата вследствие его округления по правилу II подсчёта цифр повышается. Но если, например, взять произведение $1{,}41 \cdot 1{,}73 = 2{,}4393$, считая сомножители приближениями до трёх значащих цифр к точным значениям $\sqrt{2} = 1{,}41421\ldots$ и $\sqrt{3} = 1{,}73205\ldots$, и округлить его согласно правилу II, то окажется, что это округлённое произведение 2,44 отличается от точного произведения $\sqrt{2} \cdot \sqrt{3} = \sqrt{6} = 2{,}44948\ldots$ несколько меньше, чем неокруглённое. Детальное исследование показывает, однако, что вообще округление у х у д ш а е т точность, и если бы дело было только в точности, — приближённые результаты лучше было бы вовсе не округлять. Но для вычислительной практики громадное значение имеет и п р о с т о т а результатов: отказ от округлений влечёт за собой необходимость иметь дело с числами, имеющими очень много, сплошь и рядом даже бесконечно много цифр, и вычисление становилось бы крайне трудным или даже вовсе невыполнимым.

Как можно показать, это неблагоприятное влияние округлений становится почти неощутимым, если соблюдать следующее правило:

П р а в и л о V п о д с ч ё т а ц и ф р. *Во всех промежуточных результатах* (т. е. в тех, которые служат данными для последующих действий в той же задаче) *следует сохранять не столько цифр, сколько рекомендуют правила* I—IV, *а одной больше.*

Соблюдая это правило, такую лишнюю («запасную») цифру лучше как-нибудь отмечать, например писать её в уменьшенном размере; в последнем (окончательном) результате она отбрасывается. Сохранение вместо одной двух и более запасных цифр оправдано лишь в случае особо сложных вычислений, в громадном же большинстве обычных вычислений оно бесполезно для точности окончательного результата и вредно сказывается на общем объёме работы.

Аналогичное положение имеет место в случае, когда данные имеют различное число цифр (десятичных знаков при сложении и вычитании, значащих цифр при других действиях):

П р а в и л о VI п о д с ч ё т а ц и ф р. *Более точные данные рекомендуется предварительно округлять, сохраняя в них лишь по одной лишней (запасной) цифре сравнительно с менее точными данными.*

Сохранение более чем одной лишней цифры бесполезно для точности, что доказывается сравнением значений средней квадратической погрешности результата (см. таблицу на стр. 411), и вредно из-за усложнения работы, а отказ от лишней цифры снижает точность.

Решим с применением правил подсчёта цифр задачу, решённую на стр. 395—396, со строгим учётом погрешностей. Требуется найти $t=\sqrt{a:b}$, $a=2hd$, $b=g(d-d_1)$, зная, что $h\approx 25{,}3$, $d\approx 19{,}32$, $d_1\approx 0{,}998$, $g\approx 982$.

Приводим полностью всё вычисление:

$2h$	50,6	19,32	19,32	18,322	977,6 : 17930
$a=2hd$	977,6	50,6	0,998	982	9776 : 179900 = 0,054302 ... ≈ 0,05430
$d-d_1$	18,322	11 592	18,322	36 644	8995
$b=g(d-d_1)$	17930	966 0	18,322	146 576	7810
$a:b$	0,05430	977,592		164 898	7196
$t=\sqrt{a:b}$	0,233	977,6		17992,204	6140
Ответ:	$t\approx 0{,}233$			17990	5097
					4300

$\sqrt{0{,}05430}\approx 0{,}2330$ (по таблице).

Полученный ответ находится в полном согласии с тем, что дало вычисление по способу границ (см. стр. 396, где было найдено $t\approx 0{,}2331$ ($\pm 0{,}0007$)).

Решим ещё задачу, решённую на стр. 390 по способу границ: найти $\delta=\frac{p}{v}$, $v=\pi r^2 h$, если $2r\approx 0{,}048$ *см*, $h=26{,}44$ *см*, $p\approx$ $\approx 0{,}423$ *г*. На стр. 377—378 отмечались те затруднения, какие неизбежно встают на пути решения этой простой задачи, если игнорировать особенности производства действий над приближёнными числами.

Здесь мы имеем данные $2r$, h, p с двумя, четырьмя, тремя значащими цифрами. С каким числом цифр взять $\pi=3{,}14159\ldots$? Замечая, что придётся выполнять только действия умножения и деления, применяем правило VI и ограничиваемся значением $\pi=3{,}14$. Ниже приведены полностью все выкладки, нужные для решения задачи.

$2r$	0,048
r	0,024
r^2	0,00576
π	3,14
πr^2	0,01809
h	26,44
$v=\pi r^2 h$	0,4783
p	0,423
$\delta=\frac{p}{v}$	0,88

0,00576 · 3,14

2304
576
1728
0,0180864
0,01809

0,01809 · 26,44

7236
7236
10854
3618
0,4782996
0,4783

0,423 : 0,4783
4230 : 4783 = 0,884...
42300
38264
40360
38264
20960
19132
1828

Ответ: $\delta\approx 0{,}88$.

Опять получили полное согласие с тем, что дал способ границ. Однако надо иметь в виду, что применение способа границ (как в этой задаче, так и всегда) даёт совершенно определённое указание на наибольшую возможную ошибку результата, а правила подсчёта цифр, приводя к тому же самому числовому результату, обеспечивают лишь высокую вероятность того, что погрешность последней сохранённой цифры результата невелика. Если такая неполная определённость результата представляется недопустимой, то необходим строгий учёт погрешностей, но и в таких случаях применение правил подсчёта цифр полезно, так как позволяет сделать первоначальную ориентировку в вопросе об ожидаемом числе заслуживающих доверия цифр результата и указывает, с каким числом цифр следует вести всё вычисление.

Рассмотрим ещё один пример вычисления, подтверждающий целесообразность правила округления промежуточных результатов (правило V).

При решении уравнения $f(x) = x^4 + 2x^3 - 5x^2 + 3x - 7 = 0$ найден до сотых долей один из его корней, а именно, $x_1 \approx -3{,}71$, и требуется с целью проверки найти $f(x_1)$.

Проведём вычисление (с применением правил подсчёта цифр) три раза: без запасной цифры, с одной запасной цифрой, с двумя запасными цифрами.

x	$-3{,}71$	$-3{,}71$	$-3{,}71$
x^2	$13{,}8$	$13{,}7_6$	$13{,}76_4$
x^3	$-51{,}1$	$-51{,}0_6$	$-51{,}06_4$
$2x^3$	-102	$102{,}_1$	$-102{,}_{13}$
$-5x^2$	$-69{,}0$	$-68{,}8_0$	$-68{,}82_0$
$3x$	$-11{,}1$	$-11{,}1_3$	$-11{,}13_0$
-7	$-7{,}0$	$-7{,}00$	$-7{,}000$
$2x^3 - 5x^2 + 3x - 7$	-189	$-189{,}_0$	$-189{,}_{08}$
x^4	190	$189{,}_2$	$189{,}_{45}$
$f(x)$	$+1$	$+0{,}_2$	$+0{,}_{37}$
То же по отбрасывании запасных цифр	$+1$	0	0

Как видим, сохранение одной запасной цифры несколько изменило окончательный результат. Вторая же запасная цифра никакого нового изменения этого результата не вызвала.

Остаётся указать ещё на один случай употребления запасных цифр — на вычисления с наперёд заданной точностью. Если данные можно брать с более или менее произвольным числом цифр, а точность результата наперёд указана, то, взяв данные с таким числом цифр, какое даст согласно правилам I — IV требуемое число цифр

в результате, т. е. взяв эти данные, так сказать, «в обрез», мы никогда не можем ручаться за точность последней цифры результата: правила подсчёта цифр говорят только то, что значительная погрешность в этой последней цифре гораздо менее вероятна, чем малая. Эта сомнительность последней цифры исчезает, если взять в приближённых данных по одной запасной цифре. Большее число запасных цифр, как оказывается, выигрыша точности уже не даёт, доставляя лишь добавочную вычислительную работу (конечно, в случае особо сложного вычисления лучше брать две запасные цифры).

Правило VII подсчёта цифр. *Если данные можно брать с произвольной точностью, то для получения результата с k цифрами данные следует брать с таким числом цифр, какое даёт согласно правилам* I—IV $k+1$ *цифру в результате.*

Вот пример вычисления с наперёд назначенной точностью. Пользуясь бесконечным рядом

$$\lg(1+x)=M\left(x-\frac{1}{2}x^2+\frac{1}{3}x^3-\frac{1}{4}x^4+\frac{1}{5}x^5-\ldots\right),$$

где $M=0{,}43429448\ldots$, $-1<x\leqslant+1$, найти четырёхзначный логарифм числа 7.

Взять $x=6$, чтобы сразу получить $\lg 7$, невозможно, так как ряд сходится и может быть использован для целей вычисления лишь при значениях x, меньших (по абсолютному значению) единицы. Поэтому найдём сначала $\lg 0{,}7$, для чего возьмём $x=-0{,}3$. Вычисление будем вести с одним запасным десятичным знаком, т. е. с пятью $(4+1=5)$ десятичными знаками, и возьмём все члены ряда, не обращающиеся в нуль при округлении до пяти десятичных знаков:

x	$-0{,}30000$
x^2	$0{,}09000$
x^3	$-0{,}02700$
$x^4=(x^2)^2$	$0{,}00810$
$x^5=x^2\cdot x^3$	$-0{,}00243$
$x^6=(x^3)^2$	$0{,}00073$
$x^7=x^3\cdot x^4$	$-0{,}00022$
$x^8=(x^4)^2$	$0{,}00007$
$x^9=x^4\cdot x^5$	$-0{,}00002$
$x^{10}=(x^5)^2$	$0{,}00001$
M	$0{,}43429$

x	$-0{,}30000$
$-x^2:2$	$-0{,}04500$
$x^3:3$	$-0{,}00900$
$-x^4:4$	$-0{,}00202$
$x^5:5$	$-0{,}00049$
$-x^6:6$	$-0{,}00012$
$x^7:7$	$-0{,}00003$
$-x^8:8$	$-0{,}00001$
$x^9:9$	$-0{,}00000$
S	$-0{,}35667$
MS	$-0{,}15490$

Итак, по отбрасывании запасной цифры $\lg 0{,}7=-0{,}1549$, откуда

$$\lg 7=\lg(0{,}7\cdot 10)=-0{,}1549+1=0{,}8451.$$

Именно это значение $\lg 7$ мы и находим в таблице четырёхзначных логарифмов. Напомним, что, желая провести то же вычисление со строгим учётом погрешностей, мы должны были бы принять во внимание ещё и остаточный член ряда.

Особого упоминания требует явление «потери точности при вычитании»: при вычитании двух близких друг к другу приближённых чисел, имеющих поровну десятичных знаков, в разности получается столько же десятичных знаков, число же значащих цифр получается меньшее, чем было в каждом компоненте. Поэтому, желая получить такую разность с определённым числом значащих цифр, мы должны вычислить компоненты с числом знаков, значительно бóльшим.

Пусть, например, требуется получить значение $x = \frac{\operatorname{tg}\alpha - \sin\alpha}{(\operatorname{arc}\alpha)^3}$ при $\alpha = 5°$ с тремя значащими цифрами (символом $\operatorname{arc}\alpha$ здесь обозначена радианная мера дуги α).

Для получения частного с тремя значащими цифрами делимое и делитель надо взять согласно правилу VII подсчёта цифр с четырьмя значащими цифрами. Чтобы получить разность $\operatorname{tg} 5° - \sin 5° = 0{,}0875 - 0{,}0872$ с четырьмя значащими цифрами, значения $\operatorname{tg} 5°$ и $\sin 5°$ надо взять не с четырьмя десятичными знаками, как мы сейчас их взяли, а с семью. Значение $\operatorname{arc} 5°$ достаточно взять с пятью десятичными знаками.

Вычисление понятно из приводимой схемы.

$\operatorname{arc} 5°$	0,08727
$\operatorname{tg} 5°$	0,0874887
$\sin 5°$	0,0871557
$a = \operatorname{tg} 5° - \sin 5°$	0,0003330
$b = (\operatorname{arc} 5°)^3$	0,0006646
$x = \frac{a}{b}$	0,501

В настоящем случае тот же результат можно получить гораздо легче, если предварительно преобразовать числитель данного выражения к виду, удобному для логарифмирования, и воспользоваться таблицей четырёхзначных логарифмов. Тогда

$$x = \frac{\sin 5°(1 - \cos 5°)}{\cos 5° \cdot (\operatorname{arc} 5°)^3} = \frac{2\operatorname{tg} 5° \sin^2 2°30'}{(\operatorname{arc} 5°)^3} = \frac{2\operatorname{tg} 5° \sin^2 2°30'}{(\pi : 36)^3} \text{ и } x \approx 0{,}5012$$

или по округлении до трёх десятичных знаков $x \approx 0{,}501$.

Необходимо указать ещё на одно правило, позволяющее судить о точности результата логарифмического вычисления. Вычисляя с помощью логарифмов одночленное выражение, содержащее только точные компоненты, получают результат с вычислительной погрешностью, тем меньшей, чем больше десятичных знаков имеют использованные табличные мантиссы. Причина появления погрешности понятна: все табличные мантиссы логарифмов, кроме логарифмов

чисел 1, 10, 100 и т. д., — числа приближённые. Как показывает опыт и подтверждает теоретическое исследование, вычислительная погрешность, вносимая в результат вследствие применения таблицы k-значных логарифмов, делает не вполне надёжной k-ю значащую его цифру. Вычислим, например, значение $x = 70 : 19$, пользуясь таблицами 3-, 4-, 5-, 7-, 12-значных логарифмов [1]).

k	3	4	5	7	12
lg 70	1,845	1,8451	1,84510	1,8450980	1,845098040014
lg 19	1,279	1,2788	1,27875	1,2787536	1,278753600953
lg x	0,566	0,5663	0,56635	0,5663444	0,566344439061
x	3,68	3,684	3,6842	3,684210	3,68421052632

Сравнение с точным значением

$$x = 70 : 19 = 3{,}684210526315789473 68\ldots,$$

представляющим собой периодическую дробь с периодом из 18 цифр, показывает, что все цифры полученных приближённых результатов точны. Но можно привести сколько угодно примеров вычислений посредством k-значных логарифмов, когда полученный результат отличается от точного на 1—2 единицы k-го разряда. Так, вычисление частного $17 : 6 = 2{,}833\ldots$ посредством четырёхзначных логарифмов даёт 2,832, а вычисление числа $3{,}9^3 = 59{,}319$ посредством пятизначных логарифмов даёт 59,317.

Чтобы получить с помощью логарифмов результат с k точными значащими цифрами, надо взять таблицу $(k + 1)$-значных логарифмов. Это соображение приводит к правилу VIII подсчёта цифр, указанному ниже. Соблюдая его, устраняют опасность снизить из-за применения логарифмов точность результата, достижимую при данной точности компонентов, а также опасность без нужды осложнить вычислительную работу применением логарифмов с числом десятичных знаков, слишком большим при этой их точности.

Вот сводка из восьми рассмотренных правил.

I. *При сложении и вычитании приближённых чисел в результате следует сохранять столько десятичных знаков, сколько их в приближённом данном с наименьшим числом десятичных знаков.*

Примечание. «Десятичными знаками» числа называются те цифры, которые расположены справа от знака дробности.

II. *При умножении и делении в результате следует сохранять столько значащих цифр, сколько их имеет приближённое данное с наименьшим числом значащих цифр.*

---

[1]) Двенадцатизначные логарифмы взяты по книге: М. Ф. Субботин, Многозначные таблицы логарифмов, Издательство Академии наук СССР, 1940.

Примечание. «Значащими цифрами» числа называются все его цифры, кроме нулей, расположенных левее первой отличной от нуля его цифры.

III. *При возведении в квадрат и куб в результате следует сохранять столько значащих цифр, сколько их имеет возводимое в степень приближённое число.*

Примечание. Последняя цифра квадрата и особенно куба при этом менее надёжна, чем последняя цифра основания.

IV. *При извлечении квадратного и кубического корней в результате следует брать столько значащих цифр, сколько их имеет подкоренное число* (приближённое).

Примечание. Последняя цифра квадратного и особенно кубического корня при этом более надёжна, чем последняя цифра подкоренного числа.

V. *При вычислении промежуточных результатов следует брать одной цифрой более, чем рекомендуют предыдущие правила.*

Примечание. В окончательном результате эта «запасная цифра» отбрасывается. Писать её рекомендуется в уменьшенном размере.

VI. *Если некоторые данные имеют больше десятичных знаков* (при действиях I ступени) *или больше значащих цифр* (при действиях II и III ступеней), *чем другие, то их предварительно следует округлять, сохраняя лишь одну лишнюю цифру.*

VII. *Если данные можно брать с произвольной точностью, то для получения результата с k цифрами данные следует брать с таким числом цифр, какое даёт согласно правилам* I — IV $k+1$ *цифру в результате.*

VIII. *При вычислении значения одночленного выражения посредством логарифмов следует подсчитать число значащих цифр в приближённом данном, имеющем наименьшее число значащих цифр, и взять таблицу логарифмов с числом десятичных знаков на* 1 *бо́льшим. В окончательном результате последняя значащая цифра отбрасывается.*

Примечание. При применении всех правил подсчёта цифр следует избегать нулей, помещаемых в конце приближённых чисел взамен неизвестных цифр.

ГЛАВА III

РАЗЛИЧНЫЕ ВОПРОСЫ

§ 14. Приближённые формулы. Сокращённые приёмы действий

В практических вычислениях широко используются некоторые приближённые формулы, обоснование которых вполне доступно учащимся старших классов средней школы. Так, легко проверяется тождество

$$\frac{1}{1+x} = 1 - x + \frac{x^2}{1+x},$$

показывающее, что в случаях, когда число x настолько мало, что при принятой точности вычисления его квадратом можно пренебречь, допустима замена выражения $1:(1+x)$ разностью $1-x$.

Замечая, что корни уравнения

$$\frac{x^2}{1+x} = 0{,}005$$

суть 0,0733 и $-0{,}0683$, убеждаемся, что эта замена вносит погрешность, не превосходящую половины единицы разряда второго десятичного знака (половины сотой), если x находится в интервале от $-0{,}0683$ до 0,0733, т. е. если x по абсолютному значению не превосходит 0,074. Точно так же устанавливаем, что погрешность приближённой формулы $1:(1+x) \approx 1-x$ не превосходит $0{,}5 \cdot 10^{-3}$, если $|x| < 0{,}022$, и $0{,}5 \cdot 10^{-4}$, если $|x| < 0{,}0074$. Применяя эту формулу, например, для получения частного $1:0{,}997$, когда $x = -0{,}003$, имеем $1 - x = 1 + 0{,}003$, и уверенно пишем: $1:0{,}997 \approx 1{,}0030$ (непосредственное деление даёт 1,0030090 ...). Применение приближённой формулы $1:(1+x) \approx 1-x$, как видим, существенно облегчает выполнение действия деления; что ещё важнее, — эта формула позволяет легко учесть то изменение частного, какое

получается при небольшом изменении делителя: если число Δb весьма мало по сравнению с b, то

$$\frac{a}{b+\Delta b}=\frac{a}{b\left(1+\frac{\Delta b}{b}\right)}=\frac{a}{b}\cdot\frac{1}{1+\frac{\Delta b}{b}}\approx\frac{a}{b}\left(1-\frac{\Delta b}{b}\right),$$

$$\frac{a}{b+\Delta b}-\frac{a}{b}=-\frac{a}{b}\cdot\frac{\Delta b}{b}.$$

Пренебрегая числом x^2, получаем приближённую формулу

$$(1+x)^2\approx 1+2x,$$

а заменив в этой формуле $2x$ через y и извлекая из каждой части квадратный корень, приходим к новой приближённой формуле

$$\sqrt{1+y}\approx 1+0{,}5y.$$

Приводим список простейших приближённых формул, особенно часто используемых в вычислительной практике, указывая те наибольшие значения аргумента x, при которых погрешность формулы не превышает $0{,}5\cdot 10^{-k}$ для $k=2$, 3, 4. Эти наибольшие значения устанавливаются проще всего путём непосредственного вычисления левой и правой частей при ряде возрастающих значений аргумента (с применением таблиц).

	Формула	$k=2$	$k=3$	$k=4$
I	$(1+x)(1+y)\approx 1+x+y$ $\quad\lvert x\rvert\geqslant\lvert y\rvert$	0,07	0,022	0,007
II	$(1+x)(1+y)(1+z)\approx 1+x+y+z$ $\quad\lvert x\rvert\geqslant\lvert y\rvert\geqslant\lvert z\rvert$	0,04	0,012	0,004
III	$(1+x)^2\approx 1+2x$	0,07	0,022	0,007
IV	$(1+x)^3\approx 1+3x$	0,04	0,012	0,004
V	$\frac{1}{1+x}\approx 1-x$	0,07	0,022	0,007
VI	$\frac{1}{1+x}\approx 1-x+x^2$	0,18	0,081	0,037
VII	$\sqrt{1+x}\approx 1+\frac{1}{2}x$	0,21	0,064	0,020
VIII	$\sqrt{1+x}\approx 1+\frac{1}{2}x-\frac{1}{8}x^2$	0,46	0,20	0,09
IX	$\sqrt[3]{1+x}\approx 1+\frac{1}{3}x$	0,22	0,068	0,021

	Формула	$k=2$	$k=3$	$k=4$
X	$\sqrt[3]{1+x} \approx 1 + \frac{1}{3}x - \frac{1}{9}x^2$	0,47	0,21	0,09
XI	$\sin x \approx x$	17°	8°,2	3°,8
XII	$\sin x \approx x - \frac{1}{6}x^3$	51°	32°	20°
XIII	$\cos x \approx 1$	5°,7	1°,8	0°,5
XIV	$\cos x \approx 1 - \frac{1}{2}x^2$	33°	18°	10°
XV	$\operatorname{tg} x \approx x$	14°	6°,4	3°,0
XVI	$\operatorname{tg} x \approx x + \frac{1}{3}x^3$	29°	18°	11°
XVII	$\lg(1+x) \approx 0{,}4343x$	0,15	0,048	0,015
XVIII	$\ln(1+x) \approx x$	0,10	0,031	0,010
XIX	$e^x \approx 1 + x$	0,09	0,031	0,010
XX	$10^x \approx 1 + 2{,}303x$	0,04	0,014	0,004
XXI	$\lg\frac{1+x}{1-x} \approx 0{,}8686x$	0,25	0,119	0,055
XXII	$\ln\frac{1+x}{1-x} \approx 2x$	0,19	0,090	0,042

Здесь lg означает десятичный логарифм, ln — натуральный логарифм; в тригонометрических формулах x выражен в радианной мере.

Приближённые формулы существенно облегчают работу вычисления во многих частных случаях. Эту же цель преследуют так называемые «сокращённые приёмы» производства действий умножения, деления, извлечения квадратного корня, применимые почти всегда, особенно когда данные числа — приближённые. Относительно значения этих приёмов для школы имеются весьма различные мнения. Например, проф. В. Л. Гончаров в своей книге [5] уделяет этим приёмам много внимания. Но если учесть, что эти приёмы, указанные очень давно, никакого распространения в школе не получили, хотя рекомендовались чуть не в каждой книге для учителя, посвящённой вычислительной работе, то представляется более правильным другой взгляд, согласно которому эти приёмы имеют лишь второстепенное значение по сравнению со счётными приборами и таблицами. Как бы то ни было, учителю полезно быть знакомым с ними.

Положим, требуется найти первые четыре значащие цифры произведения 29,97 · 2,738. Ниже это умножение выполнено обычным способом (слева) и «сокращённым» способом (справа).

29,97 · 2,738	29,97 · 2,738
23976	8372
8991	5994
20979	2098
5994	90
82,05786	24
82,06	82,06

Цифры множителя подписываются под цифрами множимого в обратном порядке, причём, раз требуется получить четыре значащие цифры произведения, то цифра старшего разряда множителя подписывается под четвёртой (считая слева направо) значащей цифрой множимого. Каждое частное произведение получается путём умножения (на соответствующую цифру множителя) лишь тех цифр множимого, которые выше и левее этой цифры множителя. Так, на 2 умножается число 2997, на 7 — только 299, на 3 — уже лишь 29 и на 8 — только 2. На отбрасываемые цифры множимого берётся приближённая поправка. Например, при получении второго частного произведения замечаем, прежде всего, что отбрасываемая цифра 7 при умножении на 7 даёт около 5 десятков. Запоминая эту поправку 5, умножаем 9 на 7 и к произведению 63 прибавляем 5. Получив 68, записываем 8 под крайней правой цифрой первого частного произведения, цифру же 6 запоминаем. Получение остальных цифр частного произведения идёт обычным порядком.

Для определения положения знака дробности можно дать особое правило, но проще произвести грубо приближённую оценку произведения. В данном случае, получив в произведении цифры 8206 и замечая, что сомножители близки к 30 и 3, видим, что произведением может быть только число 82,06, а никак не 8,206 или 820,6.

Записывая сомножитель так, как указано выше, мы получим либо как раз столько цифр, сколько требуется, либо одной больше. В последнем случае эту лишнюю цифру отбрасываем.

Объяснение этого приёма не представляет затруднений. Надо только сопоставить частные произведения при полном и сокращённом умножении. Погрешность результата сокращённого умножения (при точных сомножителях) не превосходит пол-единицы последнего разряда произведения, умноженной на число цифр множителя.

Переходя к сокращённому делению, рассмотрим такой пример: требуется найти четыре первые значащие цифры частного от деления 81,3747 на 0,377264. Ниже сопоставлено это деление, выполненное обычным способом (слева) и «сокращённым» (справа).

81,37	4700 : 0,377264 = 215,6 ...		813747 : 377264 = 215,7
75,45	28	= 215,7	7545
5921	90		592
3772	64		377
2149	260		215
1886	320		189
262	9400		26
226	3584		26
36	58160		0

Здесь тоже можно устранить из вычисления все цифры правее вертикальной черты. Для этого отделяем в делителе столько цифр, сколько их требуется в частном, т. е. в данном случае четыре значащие цифры, и начинаем деление обычным способом, не обращая внимания на знаки дробности в делимом и в делителе, с той лишь разницей, что после получения каждой цифры частного отбрасываем по одной (последней) цифре делителя, а последующих цифр делимого не сносим.

Разделив 8137 на 3772, получаем первую цифру частного 2. Умножив 2 на 3772 с поправкой на отброшенные цифры делителя, получаем произведение 7545 и первый остаток 592. Теперь отбрасываем последнюю цифру делителя и делим 592 уже только на 377. Получаем вторую цифру частного 1, умножаем её на 377 и находим второй остаток 215. Делим его на 37, получаем третью цифру частного 5, произведение которой на 37 с поправкой на отброшенные цифры делителя есть 189. Это даёт третий остаток 26. Остаётся разделить 26 на 3. Если возьмём в частном 8, то произведение 8 на 3 с поправкой на отброшенные цифры делителя даёт 30 и остаток — 4. Если же взять в частном не 8, а 7, то произведение 7 на 3 (с поправкой) даёт как раз 26.

Итак, цифровой состав частного установлен; остаётся выяснить положение знака дробности. Берём грубо приближённые значения делимого и делителя и замечаем, что частное должно быть близким к $80:0{,}4=200$. Поэтому ставим запятую после третьей значащей цифры и получаем окончательно в частном 215,7.

Правило сокращённого деления становится вполне понятным, если сопоставить шаг за шагом весь процесс полного и сокращённого деления.

Остаётся рассмотреть сокращённый способ извлечения квадратного корня. Он основан на следующей теореме:

Теорема. *Если по вычислении n значащих цифр корня остаток от извлечения разделить на удвоенное найденное значение корня, то частное даёт $n-1$ следующих цифр корня.*

Для доказательства предположим, что подкоренное b имеет целую часть из n граней. Пусть найдено n первых цифр корня, образующих собой число a, и надо найти дробную часть корня, которую обозначим буквой x. Таким образом,

$$\sqrt{b}=a+x,\quad b=a^2+2ax+x^2,\quad \frac{b-a^2}{2a}=x+\frac{x^2}{2a}.$$

Разность $b-a^2$ есть не что иное, как остаток, получаемый после разыскания n цифр корня, а дробь $\frac{b-a^2}{2a}$ представляет собой то самое частное, о котором говорится в тексте теоремы. Отсюда

заключаем, что

$$x = \frac{b - a^2}{2a} - \frac{x^2}{2a}.$$

Принимая $x \approx \frac{b - a^2}{2a}$, мы допускаем погрешность, равную $\frac{x^2}{2a}$. Но $x < 1$, $a \geqslant 10^{n-1}$, а потому

$$\frac{x^2}{2a} < 0{,}5 \cdot 10^{-(n-1)}.$$

Если, выполняя деление $b - a^2$ на $2a$, мы остановимся, найдя $n - 1$ десятичный знак частного, и округлим его, как обычно, то к вышенайденной погрешности прибавится ещё погрешность от округления, и полная погрешность приближённого значения корня в самом неблагоприятном случае может приблизиться к целой единице разряда $(n - 1)$-го десятичного знака, но никогда не достигнет этого предельного значения.

Если знак дробности в подкоренном числе стоит не там, где мы его предполагали, его всегда можно перенести на надлежащее место, производя умножение (или деление) подкоренного числа на некоторую степень 10 с чётным показателем, с тем, чтобы потом разделить (или умножить) найденный корень на степень 10 с показателем, вдвое меньшим. На практике делать это преобразование не нужно.

Рассмотрим пример. Положим, требуется найти $\sqrt{10}$ с 7 значащими цифрами. Обычным способом найдём первые четыре цифры; деление остатка на удвоенный корень даст следующие 3. Для сравнения помещаем рядом (справа) запись процесса получения всех семи цифр обычным способом:

$\sqrt{10} = 3{,}162277$

9	
61	100
1	61
626	3900
6	3756
6322	14400
2	12644

1756 : 6324

1265

491

443

48

44

4

$\sqrt{10} = 3{,}162277\ldots$

9	
61	100
1	61
626	3900
6	3756
6322	14400
2	12644
63242	175600
2	126484
632447	4911600
7	4427129
6324547	48447100
7	44271829

4175271

Остаток 1756 мы считали целым и делили его на удвоенное найденное число, тоже считая его целым, а полученные цифры частного просто приписали к найденной ранее части корня. В самом деле, остаток у нас равен $1756 \cdot 10^{-6}$, удвоенное найденное число $6324 \cdot 10^{-3}$, частное $0{,}277 \cdot 10^{-3}$, и оно записано у нас на надлежащем месте.

§ 15. Математические таблицы

Из разнообразнейших существующих вспомогательных средств вычисления наибольшее значение по своей распространённости, простоте и удобству имеют в настоящее время математические таблицы.

В вычислительной практике постоянно употребляются разного рода математические таблицы, представляющие собой прекрасное вспомогательное средство вычислений, чрезвычайно простое по своему устройству и употреблению, вполне общедоступное по своей дешевизне, в высокой степени гарантирующее от ошибок, доставляющее громадную экономию времени и сил.

Наибольшее распространение имеют таблицы, дающие зависимость между двумя переменными величинами (из них одна является аргументом, другая — функцией). Таковы, например, таблицы логарифмов, квадратов, кубов и т. д. Таблицы, дающие зависимость между тремя переменными («таблицы функций двух аргументов»), а тем более между бóльшим числом их, встречаются гораздо реже; примером таблицы функции двух аргументов может служить любая таблица произведений.

Более глубокое изучение вопросов, связанных с устройством и употреблением математических таблиц, выполняется с помощью особой математической дисциплины — ветви математического анализа — «исчисления конечных разностей». Начальные сведения о таблицах, вполне доступные учащимся старших классов средней школы, приведены в «Объяснениях...», имеющихся в 19-м (существенно переработанном по сравнению с предыдущими) издании «Четырёхзначных математических таблиц» В. Брадиса (1948). Более подробные сведения можно найти в книгах [2а] и [2б]. В книге [5] можно найти подробные указания об интересных и поучительных упражнениях, которые желательно ввести в школьный курс математики в связи с построением таблиц.

В школе наиболее привились таблицы логарифмов чисел и логарифмов тригонометрических функций. Отметим, что для большинства задач достаточно применять четырёхзначные таблицы, позволяющие получать результаты с четырьмя значащими цифрами (последняя не вполне надёжна). Приобретая полную беглость в обращении с таблицами четырёхзначных логарифмов; школьник должен быть ознакомлен и с употреблением более полных таблиц, желательно семи-

значных, так как иногда (правда, в школьной практике очень редко) встречаются задачи, требующие вычисления с повышенной точностью.

Кроме таблиц логарифмов, существует много других таблиц, введение которых в постоянное школьное употребление надо всемерно рекомендовать. Таковы, прежде всего, таблицы квадратов и квадратных корней, которые могут быть использованы в школе ранее других таблиц и дают ощутительную экономию времени (ведь возводить числа в квадрат и извлекать из чисел квадратные корни приходится так часто!). Заметим, что при наличии более или менее полной таблицы квадратов надобность в особой таблице квадратных корней отпадает. То же самое следует сказать о таблице кубов и кубических корней. Весьма полезны таблицы значений тригонометрических функций, которые делают во многих случаях излишним приведение к логарифмическому виду и позволяют решать треугольники в VIII классе, когда логарифмы ещё не известны. Большое применение может иметь таблица обратных значений чисел и таблица для перевода градусной меры в радианную.

Маленькую табличку произведений, содержащую произведения некоторого определённого числа на целые числа первого десятка, выгодно составлять самому всякий раз, когда это число неоднократно фигурирует как сомножитель или делитель. Такая табличка быстро получается последовательным прибавлением взятого числа, причём прибавление это следует вести до получения 10-кратного значения, что даёт хороший контроль правильности всей таблички. Таблицы длины окружности, перевода градусов в радианы и некоторые другие представляют собой не что иное, как более подробные таблицы произведений (чисел π, $\pi : 180$ и др.).

Наибольшее затруднение при пользовании любой таблицей доставляет «интерполяция», т. е. процесс получения значения функции для таких значений аргумента, какие заключаются между двумя последовательными табличными его значениями, а также обратный процесс. Это «чтение между строками таблицы» обычно производится на основе предположения о равномерности изменения функции в промежутке между двумя табличными её значениями. Обыкновенная «линейная» интерполяция допустима лишь в том случае, когда последовательные табличные значения функции, соответствующие равноотстоящим значениям аргумента, имеют равные или очень медленно изменяющиеся разности («табличные разности»). Только ясное понимание существа линейной интерполяции и условия её допустимости обеспечивают сознательное, а не механическое использование таких весьма полезных и широко используемых вспомогательных средств линейной интерполяции, как «пропорциональные части» (*PP*) и «готовые поправки». Необходимо добиваться, чтобы учащиеся умели не только пользоваться такими готовыми поправками, но и сами умели их составить, что вполне достижимо даже на основании тех кратких указаний, какие приведены в «Объяснениях...».

§ 16. Графические вычисления

В тех случаях, когда достаточна точность в 2—3 значащие цифры, вычисление результата очень часто бывает возможно заменить его построением или даже простым отсчётом по готовому чертежу. Такие графические способы решения вычислительных задач, в десятки и даже сотни раз сокращающие работу вычислителя, получили в настоящее время самое широкое применение во всех отраслях техники, особенно в тех случаях, когда скорость получения числовых результатов имеет первостепенное значение. Средняя школа существенно облегчила бы труд своих выпускников, направляющихся в вузы и военные, а также военно-морские учебные заведения, по части усвоения применяемых там графических методов, если бы культивировала простейшие приёмы графических вычислений, вполне доступные даже учащимся семилетней школы. Однако с методической стороны графические вычисления в школе разработаны очень мало, и надеяться на сколько-нибудь широкое и планомерное их внедрение в среднюю школу в ближайшем же времени не приходится. Можно только настойчиво рекомендовать каждому преподавателю относительно всякой вычислительной задачи ставить вопрос о возможности упрощённого её решения графическим способом и о той выгоде, какую способ этот представляет сравнительно с обычным вычислением. Особенно подчёркиваем последнее обстоятельство — необходимость выяснения преимуществ графического решения в каждом отдельном случае. Графически решать можно любую вычислительную задачу, но иногда такое решение доставляет выигрыш, иногда нет. Решая графическим способом задачу, которая проще решается обычным вычислительным путём, мы только скомпрометируем графический способ в глазах учащихся.

Особенно бросаются в глаза выгоды графического способа в так называемых «массовых» вычислениях, когда приходится по одной и той же формуле производить вычисление много раз, пользуясь различными значениями входящих в формулу величин. Рассмотрим один простой пример.

Положим имеется ряд чисел 18, 23, 38, 57, 85, 92, представляющих собой цены в рублях разных товаров, причём требуется каждое из них уменьшить на 27%. Вычислительное решение сводится к умножению каждого из данных чисел на 0,73 и при наличии таблицы произведений или подходящего счётного прибора выполняется сразу. Но очень просто выполнимо и графическое решение, сводящееся к построению на куске клетчатой (лучше миллиметровой) бумаги прямоугольного треугольника с катетами 100 *мм* и 73 *мм* (рис. 7) и к ряду отсчётов, дающих такие сниженные цены: 13; 17; 28; 42; 62; 67 (таблица произведений даёт точные их значения 13,14; 16,79; 27,74; 41,61; 62,05; 67,16).

Миллиметровая бумага обеспечивает удобный графический способ решения задач, относящихся к линейным функциям $y = ax + b$. Выпускаемая в продажу «логарифмическая бумага» позволяет столь же просто решать задачи, относящиеся к степенным функциям вида $y = ax^{\alpha}$, где a и α — любые действительные числа, так как на такой бумаге график этой функции есть прямая линия. Применяя «полулогарифмическую бумагу», получаем возможность изображать прямыми линиями

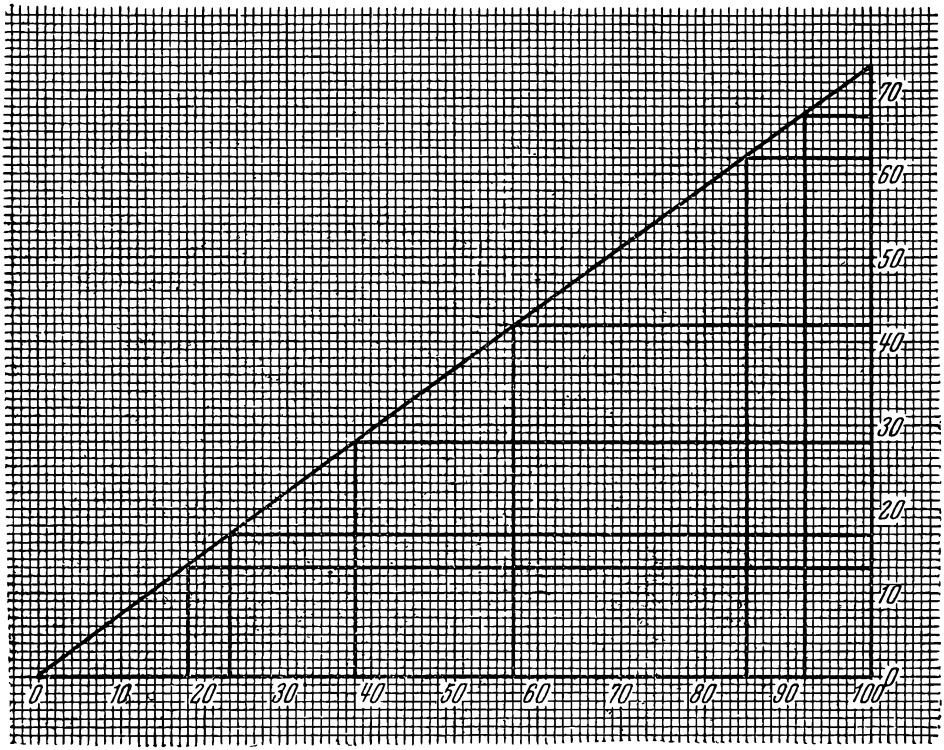


Рис. 7.

показательные и логарифмические функции $y = ab^x$ и $y = a \lg x + b$ (детали можно найти в книге [26]).

Стремление облегчить производство такого рода массовых вычислений привело к созданию целой новой отрасли математики — номографии, которой посвящён ряд книг [1]). Для первого ознакомления рекомендуем книгу [13]; некоторые немногие примеры, особенно пригодные для использования в школе, можно найти

[1]) О применении номографии к приближённому решению уравнений см. Э. э. м., кн. 2, А. П. Доморяд, Численные и графические методы решения уравнений.

в книге [26]. Желающих ознакомиться с номографией основательнее отсылаем к книге [14].

Решая одну и ту же задачу и вычислительным и графическим способами, мы приучаем учащихся к хорошему самоконтролю, так как применение графического способа легко обнаруживает грубые просчёты. С графического решения, дающего, вообще говоря, менее точные результаты, чем вычислительный, рекомендуется начинать, чтобы знание более точного значения искомого результата не толкало невольно на «подгонку» получаемого с графика менее точного результата. Так и сделано выше в § 3 при решении геометрической задачи (см. стр. 364).

§ 17. Счётная логарифмическая линейка

Несомненно, самая настоятельная задача средней школы по части рационализации вычислительной работы заключается в настоящее время в освоении теории и практики счётной логарифмической линейки. Этот простой по устройству, небольшой по размерам и в силу этого портативный, вполне общедоступный по цене счётный прибор позволяет с очень большой скоростью получать произведения, частные, степени, корни, значения логарифмов, значения тригонометрических функций, а также результаты вычисления по более сложным формулам. Счётная линейка нормальной длины, т. е. имеющая шкалы длиной в 250 *мм*, доставляет результаты с тремя значащими цифрами, а в случаях, когда число имеет первой значащей цифрой единицу, — даже четыре. Делать сложение и вычитание линейка не помогает, поэтому желательно комбинировать её со счётами. Она даёт результаты быстрее, чем арифмометр, причём выигрыш в скорости особенно значителен при массовых вычислениях. Так, например, вычисление значений $s = 4{,}9\,t^2$ для ряда значений t, хотя бы для значений t от 3 до 7 через 0,5, выполняется на линейке в течение 30—40 секунд и даёт такие результаты:

$t =$	3	3,5	4	4,5	5	5,5	6	6,5	7
$s =$	44,1	60,0	78,4	99,2	122,4	148,0	176,4	207	240.

Если работают двое, причём один манипулирует с линейкой, а другой записывает под диктовку первого полученные результаты, работа ускоряется ещё примерно на 30%.

Линейка даёт, как уже отмечено, ограниченную точность результатов, и это, естественно, делает её непригодной, например, для финансовых вычислений, где сплошь и рядом приходится иметь дело с числами, содержащими по 6, 7, 8 и больше цифр, причём вычисление ведётся с точностью до копеек, как бы велика ни была сумма. Другое дело — технические вычисления, где в подавляющем большинстве случаев интерес представляют только первые три

значащие цифры результата, нередко даже лишь две. Здесь эта ограниченная точность доставляемых линейкой результатов даже выгодна, так как все (или почти все) подлежащие отбрасыванию (как не заслуживающие доверия) цифры сами собой, механически, отпадают. Естественно, что линейка получила в настоящее время самое широкое распространение. Без неё у нас не обходится ни один инженер, ни один техник, ни один студент технического вуза, по крайней мере при работе над дипломным проектом.

Средняя школа не даёт в настоящее время никаких сведений о линейке, хотя был период, когда изучение её устройства и употребления предусматривалось обязательной программой. Неудача попытки введения линейки в школу была обусловлена тем, что, во-первых, школа не была снабжена достаточно дешёвыми и удовлетворительными по качеству счётными линейками и, во-вторых, тем, что большинство учителей математики обращаться с линейкой не умеют: в педвузах изучению линейки до последнего времени никакого внимания не уделялось. Первая причина с течением времени постепенно отпадает: в магазинах всё чаще появляются удовлетворительные по качеству недорогие линейки. Тем более досадной является вторая причина. В тех случаях, когда учитель, хорошо владеющий приёмами работы с линейкой и правильно оценивающий её значение, предлагает желающим заниматься изучением линейки в порядке дополнительной (хотя бы кружковой) работы, обычно подбирается группа учащихся, имеющих свои собственные линейки и успешно приобретающих прочные навыки в её использовании.

Существует большое число руководств, излагающих теорию логарифмической линейки и указывающих пути скорейшего овладения соответствующими навыками; главы, посвящённые линейке, имеются и в большинстве книг по технике вычислений вообще. Приводим начало главы «Счётная логарифмическая линейка» из книги автора [2а], разъясняя тем самым основную идею этого прибора и сообщая сведения, необходимые для первых шагов работы с ним.

Если взять две обыкновенные миллиметровые линейки длиной, например, по 30 *см* каждая, то без труда получим прибор для механического производства сложения и вычитания целых чисел не выше 300 при условии, что и результат не превосходит этой границы. В самом деле, расположив линейки так, чтобы их кромки со штрихами совпали, изменим нумерацию штрихов верхней линейки, написав 0 вместо 30, 1 вместо 29 и т. д. Мы получим теперь две совпадающие миллиметровые шкалы, изображённые на рис 8, *А*. Хотя цифровые метки поставлены лишь около штрихов, означающих целые сантиметры, мы можем говорить о метке каждого штриха, каждой шкалы и даже о метке каждой точки, расположенной между двумя смежными штрихами. Так, метка длинного штриха, расположенного между штрихами с метками 2 и 3, есть 2,5, ближайшего справа 2,6, следующего 2,7. Метка точки, находящейся на середине

расстояния между этими двумя штрихами, есть 2,65 и т. д. Таким образом, метка каждой точки выражает в сантиметрах её расстояние от начала шкалы. Краткости ради вместо «точка с меткой a» будем говорить просто «метка a».

Сдвинув одну из двух полученных совпадающих шкал (положим, нижнюю) вправо так, чтобы её начало оказалось против, например, метки 2,8 верхней шкалы (рис. 8, *Б*), мы будем иметь против каждой метки a нижней шкалы метку $a+2{,}8$ верхней шкалы и выполним, следовательно, сложение 2,8 с любым числом (в пределах шкалы). Например, взяв метку 4,6 на нижней шкале, читаем на верхней шкале метку 7,4, дающую сумму $4{,}6+2{,}8$. Взяв метку 5,9 на нижней шкале, читаем на верхней шкале метку $8{,}7=5{,}9+2{,}8$ и т. д.

Если, далее, требуется вычесть, например, 3,7 из 8,2, достаточно найти метку 8,2 на верхней шкале и установить против неё метку 3,7

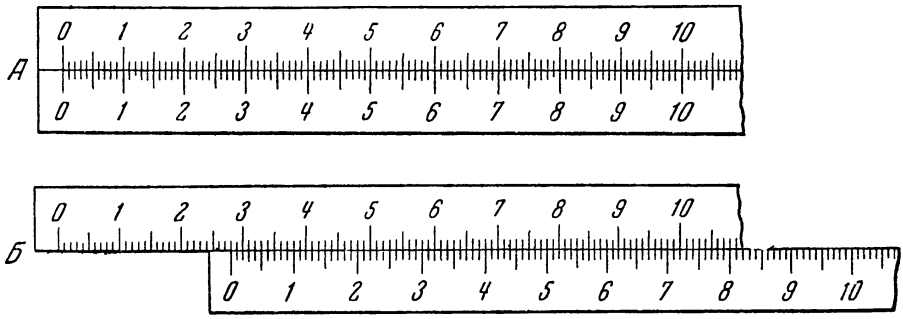


Рис. 8.

нижней шкалы. Начало нижней шкалы окажется при этом против метки 4,5 верхней шкалы, дающей разность $8{,}2-3{,}7$.

Таким образом, имеем следующие два правила: 1) чтобы найти сумму $c=a+b$, надо взять метку a на одной шкале, поставить против неё начало второй шкалы, взять на этой второй шкале метку b и прочесть противостоящую ей метку c первой шкалы; 2) чтобы найти разность $d=a-b$, надо взять метку a на одной шкале, поставить против неё метку b второй шкалы, перейти к началу этой второй шкалы, прочесть противостоящую метку первой шкалы.

Действия сложения и вычитания так просты сами по себе и так хорошо выполняются посредством конторских счётов, что только что рассмотренный прибор, который можно назвать счётной метрической линейкой, вряд ли может иметь какое-нибудь практическое значение. Однако развитие его основной идеи сопоставления двух шкал приводит к ряду других форм счётной линейки, из которых одна, носящая название «счётной логарифмической линейки», оказалась имеющей громадную практическую ценность и получила за последние десятилетия самое широкое распространение

среди всех, кому приходится производить какие бы то ни было числовые расчёты.

В счётной метрической линейке сопоставляются две метрические шкалы, где расстояние каждой точки от начала шкалы пропорционально метке этой точки. Если, сохраняя метки штрихов, передвинуть самые штрихи по шкале так, чтобы расстояние каждого штриха от начала шкалы стало пропорциональным логарифму соответствующей метки (при некотором основании), то мы получим так называемую *логарифмическую шкалу*. Обозначая буквой a метку штриха, поставленного на расстоянии в $\bar{a}$ *мм* от начала шкалы, имеем формулу $\bar{a} = m \lg a$, которую называют «уравнением логарифмической шкалы» (здесь m — коэффициент пропорциональности, который будем именовать «модулем» данной шкалы). При любом m метка 1 находится в начале шкалы, так как $m \lg 1 = 0$, метка 10

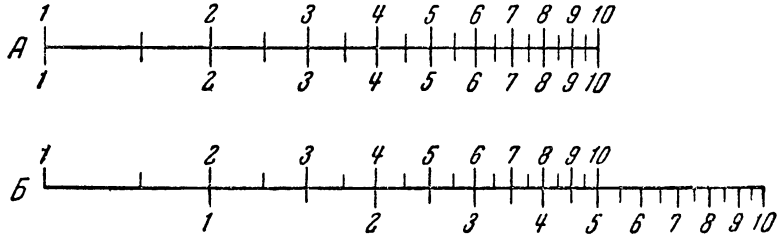


Рис. 9.

на расстоянии m *мм* от начала, метка 100 на расстоянии $2m$ *мм* от начала и т. д. Отрезок такой шкалы со штрихами, соответствующими значениям a от 1 до 10 при $m = 100$ показан на рис. 9, *А*.

При $m = 100$ *мм* штрих с меткой 1,5 находится на расстоянии $100 \lg 1{,}5 = 17{,}6$ *мм*, штрих с меткой 2 — на расстоянии $100 \lg 2 = 30{,}1$ *мм* от начала и т. д. Штрихи продолжены и вверх и вниз, чтобы, разрезав эту двойную шкалу по её оси, получить две тождественные логарифмические шкалы. Сдвигая одну из них относительно другой так, чтобы её начало, т. е. точка 1, оказалось, например, против метки 2 другой шкалы (рис. 9, *Б*), мы увидим, что против каждой метки a нижней шкалы теперь находится метка $b = 2a$ верхней шкалы. Мы таким образом выполнили умножение любого числа (в пределах шкалы) на 2.

Легко понять, почему это так. Если против метки a верхней шкалы поместить начало нижней, то против метки b нижней шкалы окажется какая-то метка c верхней (рис. 10). Отрезки $\bar{a}$, $\bar{b}$, $\bar{c}$, взятые от начала соответствующей шкалы до меток a, b, c, связаны соотношением $\bar{a} + \bar{b} = \bar{c}$, а самые метки — соотношением $m \lg a + m \lg b = m \lg c$ или $\lg a + \lg b = \lg c$ или $ab = c$. Если же против метки a верхней шкалы поместить метку b нижней (рис. 10), то против

начала нижней шкалы окажется метка c верхней, причём связь между отрезками выражается соотношением $\overline{a} - \overline{b} = \overline{c}$, а между метками — соотношением $m \lg a - m \lg b = m \lg c$ или $\frac{a}{b} = c$.

Теперь можно формулировать правила выполнения действий умножения и деления посредством пары тождественных логарифмических шкал, совершенно аналогичные правилам сложения и вычитания посредством пары метрических шкал, формулированных выше: 1) чтобы найти произведение $c = ab$, надо взять метку a на одной шкале, поставить против неё начало второй шкалы, взять на этой второй шкале метку b и прочесть противостоящую ей метку c первой шкалы; 2) чтобы найти частное $c = \frac{a}{b}$, надо взять метку a на одной шкале, поставить против неё метку b второй шкалы, перейти к началу этой второй шкалы, прочесть противостоящую метку c первой шкалы.

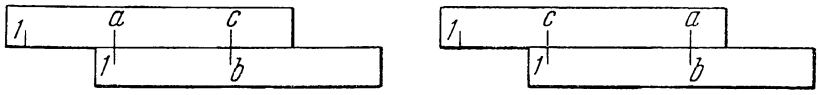


Рис. 10.

Как видим, эта пара логарифмических шкал представляет собой, прибор, позволяющий механически производить умножение и деление с той же лёгкостью, с какой метрическая счётная линейка позволяет производить сложение и вычитание. Этот счётный прибор и есть логарифмическая счётная линейка.

Уяснив идею счётной логарифмической линейки, нетрудно разобраться во всех деталях устройства и употребления такой линейки фабричного изготовления. Она отличается от только что описанной самодельной, во-первых, тем, что её шкалы исполнены очень тщательно и содержат большое число штрихов, и, во-вторых, тем, что, кроме одной пары тождественных логарифмических шкал, она имеет ещё несколько шкал, позволяющих, кроме умножения и деления, выполнять ещё целый ряд математических операций: возведение в степень, извлечение корня, решение треугольников, разыскание логарифмов, антилогарифмов и т. д.

Счётные линейки изготовляются различных размеров (карманные длиной 125 и 250 *мм*, настольные длиной 500 *мм*, демонстрационные длиной до 2 *м* и другие) и различных систем как общего назначения, т. е. для выполнения действий умножения, деления и других, так и специального назначения — для электротехников, теплотехников, артиллеристов и т. д. Наибольшее распространение и значение имеют в настоящее время «нормальные» линейки с шестью или семью шкалами длиной в 250 *мм*. Такие линейки изготовляются у нас,

в СССР, нескольких марок: «Прометей», «Металлометр» и др. Нормальные линейки позволяют находить результаты обычно с тремя, иногда с четырьмя значащими цифрами. В подавляющем большинстве технических расчётов эта точность вполне достаточна. При умелом пользовании линейка даёт огромный выигрыш и во времени, требуемом для выполнения вычисления, и в надёжности результатов, и в затрате сил. Естественно, что линейка завоевала себе столь широкое распространение: ни один инженер или техник, ни один студент технического вуза не могут в настоящее время обойтись без этого вспомогательного средства вычисления. Правда, работа на линейке предъявляет высокие требования к глазам: лицам со слабым зрением она не рекомендуется (простая близорукость, однако, ничуть не препятствует работе на линейке). Пользование линейкой при плохом освещении недопустимо.

В деле изучения линейки следует различать две ступени: первую, состоящую в овладении техникой производства действий умножения, деления, возведения в квадрат и куб, извлечения квадратного и кубического корней, решения пропорций, вычисления ряда значений, прямо или обратно пропорциональных данным, и вторую, включающую ряд более сложных операций, в том числе все тригонометрические вычисления. На полное освоение первой ступенью требуется от 15 до 20 часов работы, примерно столько же на вторую. Эта довольно значительная затрата времени быстро окупается той экономией, какую применение линейки даёт всякому вычислителю.

Вот цитата из книги «Мои воспоминания» Героя социалистического труда акад. А. Н. Крылова (Издательство Академии наук СССР, 1945, стр. 116):

«Приступив в 1892 году к чтению курса теории корабля ..., я предпослал этому курсу основания о приближённых вычислениях вообще и в приложении к кораблю в частности, выставляя как принцип, что вычисление должно производиться с той степенью точности, которая необходима для практики, причём всякая неверная цифра составляет ошибку, а всякая лишняя цифра — половину ошибки. Насколько практика этого дела была несовершенна, я показал на ряде примеров, где 90% было таких лишних цифр, которые без ущерба для точности результата могли быть отброшены, а в одном вычислении, исполненном в чертёжной Морского технического комитета, такой напрасной работы было 97%. Затем долголетней практикой я убедился, что если какая-либо нелепость стала рутиной, то чем эта нелепость абсурднее, тем труднее её уничтожить».

Эти лишние цифры, каждая из которых, по выражению А. Н. Крылова, составляет половину ошибки, радикально устраняются постоянным применением правил подсчёта цифр, о которых была речь выше (§§ 10—13). Весьма действенным средством борьбы с этими лишними цифрами является широкое применение счётной линейки.

§ 18. Вычислительная работа в разные годы обучения

В объяснительной записке к ныне действующей программе математики средней школы РСФСР читаем: «Связь теории с практикой в процессе преподавания математики осуществляется, во-первых, путём выполнения упражнений, дающих некоторую подготовку к разрешению практических вопросов, и, во-вторых, путём выполнения самих практических работ, где находят применение математические знания учащихся. Эти работы и упражнения должны быть органически связаны с программным материалом и не должны нарушать системы математических знаний» (издание 1950 г., стр. 5).

Учитель, желающий серьёзно выполнить это в высшей степени важное требование программы, желающий научить решать математические задачи, действительно встречающиеся в сельском хозяйстве, в разных отраслях техники, в военном деле, задачи, примерный перечень которых приведён в объяснительной записке, встречается с двумя затруднениями. Первое заключается в том, что такие задачи, вообще говоря, требуют больших числовых выкладок, отнимающих много времени и не имеющих никакой образовательной ценности, коль скоро навык в рациональном выполнении этих выкладок уже приобретён. Второе затруднение обусловлено приближённым характером чисел, с которыми приходится иметь дело при решении таких «реальных» задач. Точные данные встречаются в них лишь в виде исключений, а приближённые данные приводят к приближённым же результатам. Неизбежен вопрос: что́ в этих результатах заслуживает доверия? Округления, производимые без надёжной опоры в виде того или иного способа строгого учёта погрешностей или в виде хотя бы правил подсчёта цифр, таят в себе опасность либо указывания чисел с заведомо неверными цифрами («очковтирательство» из-за создания иллюзии точности!), либо отбрасывания верных цифр, т. е. неоправданного снижения точности результатов. По многовековой традиции школьная математика игнорирует этот приближённый характер большинства числовых результатов, выражающий значения реальных величин, и в этом — одна из причин оторванности школьной математики от жизни.

Как устранить эти два затруднения? Необходима рационализация вычислительной работы школьников, состоящая, во-первых, в использовании различных способов и средств, облегчающих и ускоряющих выполнение арифметических операций над многозначными числами (устный счёт, улучшение техники письменного счёта, широкое использование счётных приборов, таблиц, графиков), и, во-вторых, в усвоении элементов теории приближённых вычислений. Радикальное улучшение существующего положения требует некоторой перестройки школьной программы, но и в рамках существующей программы возможно дать учащимся много ценных и прочных сознательных навыков.

Устным счётом и улучшением техники письменных вычислений необходимо заниматься уже в V классе, заботясь о сохранении и пополнении приобретённых навыков во все последующие годы. Вычисления на счётах рекомендуются программой для V класса, и следует очень сожалеть, что ими большинство учителей пренебрегает. Вычисления на счётах можно рассматривать как первый шаг в деле механизации счётной работы, существенно облегчающий выполнение действий сложения и вычитания многозначных чисел. Второй шаг в этом направлении представляет собой введение палочек Непера, в такой же мере облегчающих действия умножения и деления многозначных чисел. В действующей программе средней школы упоминания о палочках Непера, к сожалению, нет, и пока приходится рекомендовать работу по их изготовлению и применению как дополнительную и необязательную (особые задания для более сильных учащихся, кружковая работа). Следующий шаг, являющийся уже переходом от «малой механизации» счёта к «большой» его механизации — освоение арифмометра. Это — прекрасная тема для занятий в кружке, осуществимая, если учитель даст себе труд достать экземпляр арифмометра и сам научится на нём работать.

Ещё важнее введение в школе счётной логарифмической линейки, так естественно связываемое с курсом математики IX класса. В программе требования изучать линейку пока нет, но молодёжь на многочисленных примерах видит применение линейки работниками многих специальностей, легко достаёт линейки, охотно отзывается на приглашение работать в кружке по её изучению. Попав через пару лет во втуз, знающий линейку получает большое преимущество перед незнающими, да и в средней школе линейка экономит время на производство вычислений по математике и физике. Пожалуй, нет ни одной другой частной задачи в деле улучшения постановки преподавания математики, столь насущно важной и столь легко разрешимой, как прочное введение в школьный обиход счётной линейки.

Мало используются школой и математические таблицы. Будучи вспомогательным средством вычисления, таблица должна применяться всякий раз, когда основной способ выполнения того или другого действия усвоен, а встречающиеся задачи требуют многократного производства этого действия. Первыми таблицами, с которыми можно знакомить школьников, являются таблицы произведений. Уже маленькая самодельная табличка произведений (какого-либо числа на все однозначные) серьёзно помогает при выполнении умножения и деления. Далее, приходится рекомендовать таблицы квадратов и квадратных корней, которые найдут себе применение в VI и VII классах. Аналогичная таблица кубов, позволяющая находить и кубические корни, позволит поставить много хороших геометрических задач вполне реального содержания. Широкие возможности открывает также введение таблиц длины окружности, площади круга, радианной меры, обратных значений. Успешные занятия пропедевти-

кой тригонометрии в VIII классе немыслимы без использования таблиц натуральных синусов и тангенсов. Таблицам логарифмов чисел и таблицам логарифмо-тригонометрическим школа уделяет достаточно внимания и сейчас.

Крайне важно, чтобы с самого начала имело место не механическое, а вполне сознательное пользование таблицами. Надо дать понятие о том, как таблица составлялась; хорошо произвести перевычисление хотя бы некоторых табличных данных (при рациональном разделении труда эта работа получает характер проверки готовой печатной таблицы или некоторой её части). Необходимо добиться вполне сознательного выполнения операции интерполирования и только после этого научить пользоваться вспомогательными средствами линейной интерполяции (пропорциональными частями, готовыми поправками).

Не требует ли ознакомление с таблицами лишнего времени, которого учителю математики так часто нехватает? Со введением таблиц дело обстоит так же, как и со всяким видом рационализации какой бы то ни было работы: час-другой, какие приходится затратить на ознакомление с новой таблицей, с избытком окупаются благодаря доставляемой этой таблицей экономии времени и сил. Вычисление квадратного корня с четырьмя значащими цифрами, требующее при применении обычного способа письменного вычисления двух-трёх минут, производится при помощи четырёхзначной таблицы квадратов или квадратных корней в 10—15 секунд, да и ошибки при применении таблицы встречаются гораздо реже. А сколько таких вычислений может быть облегчено благодаря таблицам!

Часто рекомендуют прививать в школе так называемые «сокращённые» способы производства арифметических действий (см. выше, стр. 423). Позволительно сомневаться в целесообразности этого. Дело в том, что выгоды от их применения становятся ощутимыми только при данных, имеющих много цифр, но такие данные в задачах практического характера встречаются крайне редко. При вычислениях же с 2-, 3-, 4-значными числами способы сокращённого производства действий не выдерживают конкуренции с различными вспомогательными средствами вычисления (таблицы, счётные приборы, графики). Это отрицательное отношение к сокращённым способам отнюдь не следует распространять на приближённые формулы (см. выше, § 14) и на различные частные приёмы производства арифметических действий, о которых речь шла в § 2.

О недооценке в школе графических вычислений была уже речь выше (§ 16). Графические вычисления доступны буквально во всех классах, и в высшей степени полезно ставить вопрос о целесообразности их применения для каждой вычислительной задачи. Вот, например, задача, для решения которой выгодно использовать график, вычерченный на кусочке клетчатой бумаги: сколько процентов их общей суммы составляют такие-то данные числа? Не зная ещё

главы о подобии фигур, легко понять возможность пропорционального изменения отрезков посредством параллельного переноса стороны треугольника.

Введение элементов теории приближённых вычислений можно рекомендовать осуществлять следующим образом. В V классе в связи с повторением мер неизбежно возникает и вопрос об измерениях. Естественно здесь же ввести и понятие приближённого значения как результата измерения, а также установить доступные школьникам приёмы обработки результатов измерений (см. выше, § 7). Дальше, естественно, появляются и простейшие правила подсчёта цифр (см. выше, § 10), целесообразность которых устанавливается доступным для пятиклассников образом на частных примерах с заменой неизвестных цифр знаками вопроса. Наибольшее значение здесь имеет просто понимание значения этих правил самим учителем и постоянство в требованиях их применения. Правила подсчёта цифр, неизбежно вытекающие из основного требования писать только заслуживающие доверия цифры («принцип академика А. Н. Крылова»), образуют первый, практически важнейший круг сведений по приближённым вычислениям.

Второй их круг образует простейший способ строгого учёта погрешностей — способ границ (см выше, § 8). По идейному своему содержанию этот способ доступен и в V классе, но лучше первое знакомство с ним отложить до VI класса, возвращаясь к нему в дальнейшем и уделяя ему особое внимание при изучении неравенств.

Третий круг сведений по приближённым вычислениям — способ границ абсолютных и относительных погрешностей. Его желательно отнести уже на VII год, притом ограничиваясь только понятием об этих границах. Оканчивающие семилетнюю школу должны понимать смысл таких выражений, как $134\ (\pm 1)$ *мм* или $5{,}4\ (\pm 2\%)$, и уметь выражать в такой форме результаты своих измерений (и своих вычислений, произведённых по способу границ). Знакомство же с теоремами о границах погрешностей результатов действий, не предусмотренное программой, но крайне желательное ввиду их приложений на занятиях в физической лаборатории, относится уже к старшим классам средней школы. Располагая этими теоремами, можно вернуться к правилам подсчёта цифр и дать новое их обоснование, пользуясь связью числа десятичных знаков с границей абсолютной погрешности, а числа значащих цифр — с границей относительной погрешности (см. выше стр. 405 и статью [6]). Если способ границ основательно усвоен, вывод теорем о границах абсолютных и относительных погрешностей проводится очень легко. Осложнение возникает лишь при отбрасывании «весьма малых чисел второго порядка малости», но если учащиеся уже знакомы с приближёнными формулами, то и этот пункт проходит благополучно.

Во всякой работе приходится различать планирование и исполнение. Доведение до конца любой математической задачи практического

содержания требует более или менее значительных численных выкладок. Эта исполнительная часть математики находится в школьном курсе математики в настоящее время на третьем или ещё более удалённом плане, и это обстоятельство не может не придавать до известной степени формальный характер всему комплексу математических знаний и навыков, выносимых учащимися из средней школы.

Чтобы преодолеть этот недостаток, необходимо, чтобы сам учитель владел теорией и практикой вычислительной работы, хотя бы в том небольшом объёме, какой указан в предыдущем изложении.

Литература

1. Берман Г. Н., Приёмы быстрого счёта, Гостехиздат, 1947.
2. Брадис В. М., а) Средства и способы элементарных вычислений, Издательство Академии педагогических наук, 1948. б) Теория и практика вычислений, изд. 5-е, Учпедгиз, 1937.
3. Филиппов А. О., Четыре арифметических действия, Издательство «Матезис», 1909.
4. Чуканцов С. М., Больше внимания технике арифметических вычислений, Математика в школе, 1948, № 4.
5. Гончаров В. Л., Арифметические упражнения и функциональная пропедевтика, Издательство Академии педагогических наук, 1947.
6. Александров П. С. и Колмогоров А. Н., Свойства неравенств и понятие о приближённых вычислениях, Математика в школе, 1942, № 2.
7. Романовский В. И., Основные задачи теории ошибок, Гостехиздат, 1947.
8. Гнеденко Б. В. и Хинчин А. Я., Элементарное введение в теорию вероятностей, изд. 2-е, Гостехиздат, 1950.
9. Кавун И. Н, Приближённые вычисления, ГИЗ, 1923.
10. Крылов А. Н., Лекции о приближённых вычислениях, издание 5-е, Гостехиздат, 1950.
11. Безикович Я. С., Приближённые вычисления, изд. 5-е, Гостехиздат, 1941.
12. Франк М. Л., Элементарные приближённые вычисления, ГТТИ, 1932.
13. Глаголев А. А., Номография для школьника, ОНТИ, 1935.
14. Глаголев Н. А., Теоретические основы номографии, ОНТИ, НКТП, 1936.
15. Панов Д. Ю., Счётная линейка, изд. 6-е, Гостехиздат, 1949.
16. Семендяев К. А., Счётная линейка, Изд. 2-е, Гостехиздат, 1950.

АЛФАВИТНЫЙ УКАЗАТЕЛЬ

Абак 46, 48, 51, 52, 53
Абацисты 53
Абсолютная погрешность 380
— —, высшая граница 380
— —, граница 380
— —, низшая граница 380
Адамар 269
Аддитивная группа поля 114
Аксиома Архимеда 131, 144, 186, 213, 224
— индукции 133, 134
— мощности 224
— полноты 224
Аксиоматическое построение математики 120, 133, 152—156
Алгебра (гиперкомплексная система) 242, 245, 246
— с делением 242, 246, 249
Алгебраические операции в группе 102, 107, 108
— — в кольце 108, 109, 112
— — в множестве 101
— числа 343
— — порядка (степени) n 343
— —, счётность множества 347, 348
Алгебры, примеры 243, 244
Алгорифм 53
— Евклида 258, 284, 291
— —, арифметические приложения 291, 292
— —, делимость многочленов 293—297
— —, — целых чисел 291—293
— — и теория измерения 291
— — и цепные дроби 299
Алгорифмики 53
Александр де Вилла Деи 53
Александров П. С. 382
ал-Каши Джиат-Эддин Джемшид 68
ал-Насави 65, 66
ал-Хассар 66
ал-Хваризми-Маго сын Мусы 53
Апексы 51
Аполлоний 12
Арганд 227
Аристотель 12, 24
Арифмометр 365, 366, 368—372
— с непрерывным движением (П. Л. Чебышева) 372
— «Феликс» 367—372
Архимед 12, 26, 36, 388, 389
Архимеда аксиома 131, 144, 186, 213, 225
Архимедовски расположенное кольцо (поле) 131

Базис векторного пространства 242, 243
Безу 286, 344
Бейер 70
Бобынин В. В. 32, 51, 55
Бойер 35
Бомбелли 227
Борель 332
Боэций 51
Бубнов Н. М. 46, 51
Бюрги 70

Вален 331
Валлис 29
Вейерштрасс 188
Векторное пространство 242
Вёпке 51
Веселовский И. Н. 43, 63
Вессель 227
Видманн 157
Виет 157
Вильсона теорема 288
Виноградов И. М. 269, 270
Выгодский М. Я. 43
Высота числа 88
Высшая граница абсолютной погрешности 380
Вычисления вспомогательные 364
—, — средства 364

Вычисления, обеспечение наперёд заданной точности результата 398
—, рациональная запись 365
—, составление схемы 364
— со строгим учётом погрешностей 388, 407
—, способ границ 388
—, — — погрешностей 392
—, точность результатов 364, 388, 400
Вычислительные машины 373
— навыки 357, 358

Галифакс (Сакробоско) 53, 55
Гамильтон 241
Ганкель 33
Гармонический ряд 265
Гаусс 227, 257, 258, 268, 284, 380
Гаусса числовое поле 251
Гельфонд А. О. 352
Геометрия чисел 339
Герберт 52
Геродот 21
Герон Александрийский 64
Грамматеус 68
Гильберт 351
Гильберта задача 351, 352
Гиперкомплексная система (алгебра) 242, 245, 246
Гиперкомплексные числа (кватернионы) 241
Гольдбаха проблема 270
Гончаров В. Л. 422
Граница абсолютной погрешности 380, 381
— — — суммы и разности 393
— относительной погрешности 381
— — — корня с натуральным показателем 395
— — — произведения 393
— — — степени с натуральным показателем 394
— — — частного 394
— — — числа $\frac{1}{b}$ 394
Графические вычисления 429, 439, 440
Графический способ вычисления, преимущества 429
Группа 102, 106
—, закон ассоциативности 102
—, — коммутативности 102
—, — обратимости 102
— подстановок 103, 104
— преобразований 103
—, примеры 102, 103
Групповая операция 107
Гурвиц 332, 351
Гюйгенс 305

Двучленные уравнения 228
Дедекинд 188
Действительная функция 214
Действительные числа 188, 202
— —, аксиоматическое определение 223—226
— —, ассоциативность сложения 223
— —, — умножения 223
— —, действия над ними 223, 224
— —, дистрибутивность умножения относительно сложения 223
— —, извлечение корня 190, 196, 197, 214, 227
— —, коммутативность сложения 223
— —, — умножения 223
— —, обратимость умножения 223
— —, представление систематической дробью 309—311
Делимость чисел 255
— —, основная теорема 256—262
Делители нуля 111, 115, 246
Десятичные знаки 419
Диофант 24, 36, 64
Диофантов (неопределённый) анализ 284
Диофантовы приближения 339
— уравнения 339
Дирихле 339
— метод 335, 339
— теоремы 269, 336—338
Дроби 57—71, 73, 179—181
— алгорифмические 59, 66
— вавилонские (шестидесятиричные) 66
— вида $\frac{1}{n}$ 57, 64
Дроби в России 66
— греческие 64
— двоичные 62
— десятичные 68—70
— — в России 70, 71
— древне-русские 62, 63
— египетские 57, 58, 62
— индусские 65
— подходящие 301
— римские (двенадцатиричные) 65
— систематические 309—314, 316
— узловые 59, 61
— цепные 298, 299, 305, 307
— шестидесятиричные 66—68, 70
Дробные числа 172, 180

Евклид 188, 259
Евклида теорема 262, 297
Единица группы 105
— кольца 115
— поля 114

Значащие цифры числа 379, 420

Измерения 383, 384, 387
Изоморфизм 122, 123, 174
Изоморфное отображение 124, 162
Интервал 82
Интерполяция 428
— линейная 428
Иоанн Севильский 53
Иррациональные числа 188, 214
— —, представление систематической непериодической дробью 316

Кантор Г. 27, 188, 206, 347, 349
Кантор М. 33, 35, 40
Кардан 68, 227
Кватерниона норма 245
Кватернион сопряжённый 245
Кватернионы (гиперкомплексные числа) 241
Кевич 40
Кеплер 70
Кирик 55
Клавишная счётная машина 373
Кобринский Н. Е. 374
Колмогоров А. Н. 382
Кольцо 108
— архимедовски расположенное 131
— — —, примеры 131, 171
—, ассоциативность сложения 109
—, — умножения 109
— вычетов по модулю 118
—, дистрибутивность умножения относительно сложения 109
—, коммутативность сложения 109
—, — умножения 109
—, обратимость сложения 109
—, порядок в нём 125, 126
—, примеры 109
— расположенное 125—128
— целых чисел 160—162, 168, 169
— — —, расположение 171
Коммутативная алгебра с делением 246
— (абелева) группа 102, 105, 107
— операция 101
Комплексные числа 227, 228
— —, аргумент 234—236
— —, геометрическое представление 233, 234
— —, деление 236, 237
Комплексные числа, извлечение корня 237—239
— —, модуль 234—236, 239, 240
— — сопряжённые 239
— —, тригонометрическая форма 234
— —, умножение 236
Компоненты вектора 242
Коши последовательность 196
Кронекер 15, 339
Крылов А. Н. 407, 436
Крылова принцип 407

Лаплас 12
Лежандр 257, 268
Лежандра теоремы 328, 330
Лейбниц 17
Леонардо Пизанский (Леонардо Фибоначчи) 54, 66
Леффлер 40
Лиувилль 343
Лиувилля теорема 344
Лобачевский Н. И. 85
Логарифмическая бумага 430
Ломоносов М. В. 55
Люстерник Л. А. 374
Ляйт 69

Магницкий Л. 66, 70
Маркс К. 16
Математическая индукция 133, 134, 144, 145
Математические таблицы 358, 427, 428
Машина для решения системы уравнений первой степени 376
— счётная клавишная 373
Машины вычислительные 373
— счётно-аналитические 374
Мера 60
Меры древнейшие 60
— древнерусские 62
Метод Дирихле 335, 339
Методы теории чисел 271—290
Миклухо-Маклай Н. Н. 22, 48
Миллиметровая бумага 430
Минковский 339, 341
Многочлен 216
— абсолютно простой (неприводимый) 294
Многочлены взаимнопростые 294
Множества бесконечные 82, 89, 94, 95
—, взаимно однозначное соответствие 86
— конечные 81, 82, 89—91, 95
— — упорядоченные 98, 99
— несчётные 92
—, операции над ними 82
— подобные 97—99

Множества, примеры 81
— равномощные (эквивалентные) 86, 87
— равные 81
— счётные 92
— упорядоченные 96
Множество 80, 81
— алгебраических чисел, счётность 347, 348
— действительных чисел 92
— натуральных чисел 88, 92
—, первый элемент 97
—, последний элемент 97
— простых чисел 262
— пустое 81
—, разбиение на классы эквивалентных элементов 159, 160
— рациональных чисел 88
— с обратным порядком 96
—, соседние элементы 97
— целых чисел 170
—, число элементов 90, 91
Мощность множества 87
Муавра формула 237
Мультиплейер 376
Мультипликативная группа поля 114

Надмножество 81, 91
— собственное 81
Надполе (расширение поля) 118
Наибольший делитель многочленов 295
— общий делитель двух чисел 291
Наилучшие приближения 324, 327
Наименьшее общее кратное двух чисел 261
Натуральные числа 11, 22, 73, 133, 262
— —, ассоциативность сложения 137
— —, — умножения 142
— —, вычитание 150, 151
— —, действия над ними 135—139, 148—152
— —, деление 151, 152
— —, дистрибутивность 141, 142
— —, коммутативность сложения 138
— —, — умножения 141
— —, монотонность сложения и умножения 143
— —, порядок 96, 135, 142—145
— —, система аксиом 133, 152—156
— —, сложение 135—138, 148
— —, умножение 139—142, 148, 149
Натуральный ряд 16, 18, 26, 27
— —, мультипликативная база 262
Нейгебауер 41—43
Неопределённый (диофантов) анализ 284
Непер 70
Непера палочки 365—367
Непрерывная дробь, см. цепная дробь
Непрерывность функции 214, 216, 217
Нессельман 67
Низшая граница абсолютной погрешности 380
Номография 430
Нулевые последовательности 209
Нуль 39, 40, 49, 51, 54
— кольца 110, 111

Область целостности 111, 169
Образ элемента 86
Обратная операция 101
Обратный элемент 105, 115
Общее кратное двух чисел 261
Объединение множеств 82, 83
Однер В. Т. 367
Одо Клюнийский 59
Округление десятичных дробей 322
— чисел по избытку 379
— — по недостатку 379
— —, правило чётной цифры 379
— результатов действий над приближёнными числами 400, 401—405, 413—417, 420
Операции над множествами 82
Относительная погрешность, граница 381
Отношение отрезков 189, 190, 196—198
Отображение множеств 85
Отрезок 82
— натурального ряда 89
Оценка результата приближённая («прикидка») 361

Палочки Непера 365—367
Пары чисел 159, 163, 164, 166, 174—177, 179, 231, 232
Паскаль 12
Пеано 133
Пересечение множеств 82, 83
Перфорационные карты 375
Планиметры 374
Погрешностей распределение 411—413
Погрешность, см. абсолютная погрешность
— большая (близкая к предельной) 411
— истинная и граница погрешности 406

Погрешность округления 322, 379
— относительная, граница 381
— предельная 400, 410
— систематическая 384
— случайная 384
— средняя квадратическая 408, 410
Подгруппа 108
Подкольцо 112, 113
Подмножество 81, 91
— собственное 81
Подполе 118, 119
Подходящие дроби 301—304
— —, приближение чисел 323—328
— —, теоремы 328—334
Позиционный принцип счисления 11, 35, 50
Поле 113
— архимедовски расположенное 181, 182, 205
— действительных чисел 202, 223
— — —, расположение и отображение 221
— комплексных чисел 228, 230
— минимальное 160, 161, 173
— непрерывное 201
— полное 198
—, примеры 114
— простое 119
— расположенное 125—128
— рациональных чисел 173—184
— — комплексных чисел 114
— характеристики $p > 0$, пример 117
— — 0 182, 183
Полуинтервал 82
Полулогарифмическая бумага 430
Последовательности стационарные 211
Последовательность элементов множества 191
— — поля ограниченная 192
— — — расходящаяся 192
— — — сходящаяся 192—194
Правила подсчёта цифр 400, 401—405, 413—417, 420
Предел последовательности элементов поля 192—195
Предельный элемент множества 225
Приближённое равенство 380
— —, точность 385
Приближённые значения 377
— —, округление результатов 378
— формулы для вычислений 421, 422, 423
— числа, возведение в квадрат, куб 404
— —, вычисление посредством логарифмов 420
Приближённые числа, извлечение квадратного и кубического корней 404
— —, округление более точных данных 414
— —, произведение 401—403
— —, промежуточные результаты действий 414
— —, сложение и вычитание 400, 401
— —, точность 381—383
— —, умножение и деление 403, 404
— —, цифры, заслуживающие доверия (точные) 381
— —, число цифр в данных 417
Приближённый результат 383
Принцип А. Н. Крылова 407—409
— счисления аддитивный 31, 48, 73
— — мультипликативный 31, 36, 45, 47, 48
— — субтрактивный (вычитания) 29, 31, 73
Прообраз элемента 86
— — полный 86
Простые числа 256, 262
— —, распределение 263, 266, 267, 269
Птолемей 67
Прошко В. М. 376

Равенство множеств 81
Равномощность множеств 86, 87
Равноостаточность чисел 273
Равноточные измерения (способ обработки результатов) 386
Радианная мера угла 216
Разность множеств 82
Расширения принцип 157—159
Рациональные числа 172, 173, 179, 180, 186—188, 299
— —, представление систематической периодической дробью 312—314
— —, единственность представления цепной дробью 299, 300
Риман 269

Сакробоско (Галифакс) 53, 55
Сечение упорядоченного множества 225
Система аксиом, независимость 155, 156
— —, непротиворечивость 153
— —, полнота 153, 154
— вычетов по модулю полная 277, 278
— — — — приведённая 278, 279
— счисления алфавитная 31—37, 73
— — аттическая (геродианова) 29, 33
— — вавилонская 39, 40, 42, 43
— — в России 55, 57

Система счисления греческая 33
— — двадцатиричная 13, 22, 31
— — двенадцатиричная 12
— — двоичная 17, 29
— — десятичная 11, 12, 22, 73
— — египетская 27—29, 31, 32, 39
— — индусская 44—46, 48, 49, 50
— — ионийская 33, 36, 37
— — китайская 31
— — позиционная 12, 13, 32, 36, 38—50, 53, 54
— — пятиричная 13, 14, 22
— — римская 14, 26, 29, 31, 33, 37
— — славянская 33, 37, 38
— — троичная 17
— — шестидесятиричная 38, 39, 40, 43
Систематическая (*k*-ичная) дробь 308
— дробь бесконечная 309
— — конечная 309, 314
— — периодическая 312
— — смешанно-периодическая 312
— — чисто периодическая 312
Систематические дроби, их преимущества 306
— —, представление чисел 309—314, 316
Системы 83
Сокращённые приёмы вычислений 422—426
— способы арифметических действий 439
Спасский И. Г. 57
Способ границ 378, 388
— — погрешностей 392—399
— — —, примеры применения теорем о границах погрешностей 395
Сравнений метод 271—290
Сравнения, сложение, вычитание, умножение, деление, степень 273—276
— алгебраические высших степеней 283, 286—290
— линейные с одним неизвестным 283—286
— содержащие неизвестные 282
— тождественные 282, 283
Сравнимость 273
Срединное значение («медиана») 385
Среднее арифметическое значение 384
— квадратическое отклонение 386
— отклонение 385
Средняя квадратическая погрешность 408, 410
Сталин И. В. 73, 74
Стевин С. 69, 70
Структурные константы (постоянные умножения) алгебры 243
Счёт 16—19, 22—25, 27, 35, 37, 48, 357
— письменный 361, 363
— полуписьменный 359
— устный 359, 438
Счётная линейка, логарифмическая шкала 434
— логарифмическая линейка 431
— метрическая линейка 432, 433
Счётно-аналитические машины 374, 376
Счётно-решающие устройства 374
— — —, моделирование 374
— — — непрерывного действия 374
Счёты русские 365, 366

Таблица разностей 375, 376
Табулятор 376
Таннери 33, 35
Тейлор 16
Тело 241
— кватернионов 244
— — рациональных 251
Теорема Евклида о бесконечности множества простых чисел 262, 297
— Лиувилля 344
— о законности индуктивных доказательств 134
— о последовательных подходящих дробях 331
— о промежуточном значении 218—220
— основная делимости чисел 257—262
— Ферма («малая») 280
— Фробениуса 249
— Чебышева 340
Теоремы Дирихле 269, 336—338
— Лежандра 328, 330
— Эйлера 264, 279
Теория чисел, методы, см. методы теории чисел
Тимченко И. Ю. 47
Тип множества 97
Толстов С. П. 52
Точность (потеря точности при вычитании) 418
— приближённого числа 381, 382
— результата логарифмических вычислений 418, 419
Точные цифры 382
Трансцендентные числа 343
— — Лиувилля 343, 345
— —, построение их 343—347, 349
Тюро-Данжен 43

Ферма́ 289
— теорема («малая») 280
Финэ 69

Фробениуса теорема 249
Фундаментальная последовательность элементов поля (последовательность Коши) 196
Функции непрерывные, примеры 216—218
— тригонометрические, определение 216, 217
Функция 84
— действительного переменного 214
— дробная рациональная 216
— заданная на множестве 85, 146
— непрерывная в точке 214, 216, 218
—, область значений 85
—, область определения 85
— $\pi(n)$ 263, 268
— $\varphi(n)$ 268, 269, 280—282
— целая рациональная 216

Характеристика поля 116, 117
— — расположенного 128
Хисс 35

Целые числа 15, 16, 57, 160, 170, 171
— — алгебраические, разложение 257
— —, классы по модулю 277
Цепные дроби 298, 299, 305, 307
— — бесконечные 315—321
— —, представление чисел 321
Цифры 50, 51, 54, 308
— арабо-индусские 52
— «губар» 50—52
— индусские 53, 55
— римские 52, 53
— славянские 55, 57

Чебышева арифмометр 372
— теорема 340
Чебышев П. Л. 255, 268, 269, 339, 372
Черепнин Л. В. 60
Числа 157, 158
Числа алгебраические 343
— алгорифмические 13, 14, 24, 25, 27
— действительные 188, 202
— дробные 172, 180
— e и π 350, 351
— иррациональные 188, 214
— количественные 140
— комплексные 227, 228
— натуральные 11, 22, 73, 133, 262
— порядковые 140
— простые 256, 262
— рациональные 172, 173, 179, 180, 186, 187, 188
— совокупности 23, 24, 47, 48
— составные 256
— сравнимые по модулю 273
— трансцендентные 343
— узловые 13, 14, 24, 25, 27, 45, 73
— целые, см. целые числа
—, понятие числа 15, 16, 18, 21, 77, 78
Числовая система йорубов 25
Числовое поле Гаусса 251
Числовой ряд 24, 25, 26, 27
Числовые знаки разных народов 28, 30
— области, конструктивное определение 223
— обозначения ацтеков 25, 31

Шнирельман Л. Г. 270
Шюке 38

Эйлера теоремы 264, 279
Эйлер Л. 255, 263, 279
Эквивалентность последовательностей 207, 208
Эквивалентные пары 175—177
Элемент множества 80
Энгельс Ф. 16, 17, 77, 121

Янжул И. Н. 376